Solucionar problemas de vSphere

Actualización 1

Modificado el 24 mayo de 2018

VMware vSphere 6.5

VMware ESXi 6.5

vCenter Server 6.5

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Acerca de solución de problemas de vSphere

En *Solucionar problemas de vSphere*, se describen la solución de problemas y los procedimientos para implementaciones de VMware vCenter Server® y componentes relacionados.

Audiencia prevista

Esta información es para cualquiera que desee solucionar problemas de máquinas virtuales, hosts ESXi, clústeres y soluciones de almacenamiento relacionadas. La información de este manual es para administradores expertos de los sistemas Windows y Linux que están familiarizados con la tecnología de máquinas virtuales y las operaciones de centro de datos.

Nota No todas las funcionalidades de vSphere Web Client se implementaron para vSphere Client en la versión de vSphere 6.5. Para obtener una lista actualizada de las funcionalidades no compatibles, consulte la *Guía sobre actualizaciones de las funcionalidades en vSphere Client* en http://www.vmware.com/info?id=1413.

Información actualizada

La documentación de *Solucionar problemas de vSphere* se actualiza con cada versión del producto o cuando es necesario.

En esta tabla se muestra el historial de actualizaciones de *Solucionar problemas de vSphere*.

Revisión	Descripción
13 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo.
24 de mayo de 2018	Se actualizó Comprobar la coherencia de los metadatos con VOMA.
4 de octubre de 2017	■ Se actualizó la información de registro en Error de tiempo de espera de TFTP de vSphere Auto Deploy durante el arranque. ■ Se actualizaron los directorios de registros en Solucionar problemas con registros.
ES-002608-00	Versión inicial.

Descripción general de la solución de problemas

1

Solución de problemas de vSphere contiene escenarios comunes de solución de problemas y ofrece soluciones para cada uno de estos. Aquí también se podrán encontrar instrucciones para resolver problemas que tienen orígenes similares. En el caso de problemas únicos, considere desarrollar y adoptar una metodología de solución de problemas.

El siguiente enfoque para solución de problemas eficaz profundiza sobre cómo solucionar problemas de información, como la identificación de síntomas y la definición del espacio problemático. También se trata la solución de problemas con archivos de registro.

Este capítulo incluye los siguientes temas:

- Directrices para solución de problemas
- Solucionar problemas con registros

Directrices para solución de problemas

Para solucionar problemas de la implementación de vSphere, identifique los síntomas del problema, determine cuáles componentes se ven afectados y pruebe posibles soluciones.

Identificar síntomas

Existen varias causas con el potencial de producir un rendimiento bajo o nulo en la implementación. El primer paso en una solución de problemas eficiente es identificar exactamente lo que está mal.

Definir el espacio problemático

Después de haber aislado los síntomas del problema, se debe definir el espacio problemático. Identifique los componentes de software o hardware que se ven afectados y que podrían estar provocando el problema y aquellos componentes que no están involucrados.

Probar posibles soluciones

Cuando sepa cuáles son los síntomas del problema y cuáles componentes están involucrados, pruebe las soluciones sistemáticamente hasta que se resuelva el problema.

Conceptos básicos de solución de problemas (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8riyfo25/uiConfId/49694343/)

Identificar síntomas

Antes de intentar resolver un problema en la implementación, es necesario identificar de forma precisa cómo es el error.

El primer paso en el proceso de solución de problemas es recopilar información que define los síntomas específicos de lo que está ocurriendo. Se podrían hacer estas preguntas cuando se recopila esta información:

- ¿Cuál es la tarea o comportamiento esperado que no está ocurriendo?
- ¿La tarea afectada puede dividirse en subtareas que se pueden evaluar por separado?
- ¿La tarea termina en un error? ¿Hay un mensaje de error asociado con ella?
- ¿La tarea se realiza pero en un tiempo prolongado inaceptable?
- ¿El error es constante o esporádico?
- ¿Qué ha cambiado hace poco en el software o hardware que podría estar relacionado con error?

Definir el espacio problemático

Después de que identifique los síntomas del problema, determine cuáles componentes en su configuración se ven afectados, cuáles componentes podrían estar provocando el problema y cuáles componentes no se ven involucrados.

Para definir el espacio problemático en una implementación de vSphere, tenga en cuenta los componentes presentes. Además del software de VMware, considere el software de terceros que hay en uso y cuál hardware se está utilizando con el hardware virtual de VMware.

Mediante el reconocimiento de las características de los elementos de software y hardware y cómo pueden influir en el problema, puede analizar problemas generales que podrían estar provocando los síntomas.

- Error de configuración de software
- Error de hardware físico
- Incompatibilidad de componentes

Divida el proceso y considere cada parte y la probabilidad de su participación por separado. Por ejemplo, un caso que está relacionado con un disco virtual en un almacenamiento local posiblemente no se relaciona con una configuración de enrutador de terceros. Sin embargo, una configuración de controladora de disco local podría estar contribuyendo al problema. Si un componente no está relacionado con los síntomas específicos, es probable que pueda eliminarlo como candidato para prueba de soluciones.

Piense en qué cambió en la configuración recientemente antes de que comenzaran los problemas. Busque lo que hay en común en el problema. Si varios problemas comenzaron al mismo tiempo, es probable que pueda hacer seguimiento de todos los problemas para la misma causa.

Probar posibles soluciones

Una vez que conozca los síntomas del problema y cuáles son los componentes de software o hardware que probablemente están más involucrados, puede probar soluciones de forma sistemática hasta que se resuelva el problema.

Con la información que ha obtenido sobre los síntomas y los componentes afectados, puede diseñar pruebas para localizar y resolver el problema. Estos consejos podrían aumentar la eficacia de este proceso.

- Generar ideas para todas las soluciones posibles que pueda.
- Comprobar que cada solución determina inequívocamente si se ha solucionado el problema o no. Probar cada posible solución pero avanzar sin demora si la solución no resuelve el problema.
- Desarrollar y buscar una jerarquía de posibles soluciones basándose en probabilidades. Eliminar sistemáticamente cada posible problema, desde el más probable hasta el menos probable, hasta que los síntomas desaparezcan.
- Cuando se prueban posibles soluciones, cambiar solo una cosa a la vez. Si su instalación funciona una vez que se hayan cambiado muchas cosas a la vez, es posible que no pueda distinguir cuál de ellas fue la que obtuvo el resultado correcto.
- Si los cambios realizados para buscar una solución no ayudan a resolver el problema, devolver la implementación a su estado anterior. Si no vuelve la implementación a su estado anterior, podrían generarse nuevos errores.
- Buscar una implementación similar que esté funcionando y probarla en paralelo con la implementación que no funciona correctamente. Haga cambios en los dos sistemas al mismo tiempo hasta que entre ellos solo haya unas diferencias o solo una.

Solucionar problemas con registros

A menudo es posible obtener valiosa información de solución de problemas revisando los registros que entregan los diversos servicios y agentes que utiliza su implementación.

La mayoría de los registros están ubicados en `C:\ProgramData\VMware\vCenterServer\Logs\`*<nombre_servicio>* en las implementaciones de Windows o en `/var/log/vmware/`*<nombre_servicio>* en las de Linux. Los registros comunes están disponibles en todas las implementaciones. Otros registros son únicos para ciertas opciones de implementación (Nodo de administración o Platform Services Controller).

Registros comunes

Los siguientes registros son comunes para todas las implementaciones en Windows o Linux.

Tabla 1-1. Directorios de registros comunes

Directorio del registro	Descripción
applmgmt	VMware Appliance Management Service
cloudvm	Registra toda la asignación y distribución de recursos entre servicios
cm	VMware Component Manager
firstboot	Ubicación donde se almacenan los registros del primer arranque
rhttpproxy	Proxy web inverso
sca	VMware Service Control Agent
statsmonitor	VMware Appliance Monitoring Service (Linux solamente)
vapi	VMware vAPI Endpoint
vmaffd	Daemon de VMware Authentication Framework
vmdird	Daemon de VMware Directory Service
vmon	VMware Service Lifecycle Manager

Registros de nodo de administración

Los siguientes registros se encuentran disponibles en caso de que se seleccione una implementación de nodo de administración.

Tabla 1-2. Directorios de registros de nodo de administración

Directorio del registro	Descripción
autodeploy	VMware vSphere Auto Deploy Waiter
biblioteca de contenido	VMware Content Library Service
eam	VMware ESX Agent Manager
invsvc	VMware Inventory Service
mbcs	Servicio de configuración de bus de mensajes de VMware
netdump	VMware vSphere ESXi Dump Collector
perfcharts	Gráficos de rendimiento de VMware
vmcam	VMware vSphere Authentication Proxy
vmdird	Daemon de VMware Directory Service
vmsyslog collector	vSphere Syslog Collector (Windows solamente)
vmware-sps	VMware vSphere Profile-Driven Storage Service
vmware-vpx	VMware VirtualCenter Server

Tabla 1-2. Directorios de registros de nodo de administración (continuación)

Directorio del registro	Descripción
vpostgres	Servicio de base de datos de vFabric Postgres
mbcs	Servicio de configuración de bus de mensajes de VMware
vsphere-client	VMware vSphere Web Client
vcha	VMware High Availability Service (Linux solamente)

Registros de Platform Services Controller

Puede analizar los siguientes registros si se selecciona una implementación de nodo de Platform Services Controller.

Tabla 1-3. Directorios de registros de nodo de Platform Services Controller

Directorio del registro	Descripción
cis-license	Servicio de licencias de VMware
sso	Servicio de token seguro de VMware
vmcad	Daemon de VMware Certificate Authority
vmdird	VMware Directory Service

Para las implementaciones de nodo de Platform Services Controller, hay registros de tiempo de ejecución adicionales que están ubicados en `C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs`.

Solucionar problemas de máquinas virtuales

2

Los temas de solución de problemas de máquinas virtuales ofrecen soluciones a posibles problemas que se podrían encontrar al usar las máquinas virtuales.

Este capítulo incluye los siguientes temas:

Solucionar problemas de máquinas virtuales con Fault Tolerance

Para mantener un alto nivel de rendimiento y estabilidad para las máquinas virtuales con Fault Tolerance y también minimizar los índices de conmutación por error, debe estar al corriente de ciertos temas sobre solución de problemas.

Los temas de solución de problemas que se tratan se centran en problemas que se podrían encontrar al usar la característica vSphere Fault Tolerance en las máquinas virtuales. En los temas también describe cómo resolver problemas.

También puede ver el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1033634 para ayudar a solucionar problemas de Fault Tolerance. Este artículo contiene una lista de mensajes de error que podría encontrarse cuando se intenta usar la característica y, cuando corresponda, asesoría sobre cómo resolver cada error.

Hardware Virtualization (Virtualización de hardware) no habilitada

Debe habilitar Hardware Virtualization (HV) (Virtualización de hardware (HV)) antes de usar vSphere Fault Tolerance.

Problema

Cuando intenta encender una máquina virtual con Fault Tolerance habilitado, podría aparecer un mensaje de error si no ha habilitado HV.

Causa

A menudo, este error es producto de que HV no está disponible en el servidor de ESXi en el que está intentando encender la máquina virtual. Puede que HV no esté disponible porque no es compatible con el hardware del servidor de ESXi o debido a que HV no está habilitado en el BIOS.

Solución

Si el hardware del servidor ESXi es compatible con HV, pero HV actualmente no está habilitado, habilítelo en el BIOS en ese servidor. El proceso para habilitar HV es diferente según los BIOS. Consulte la documentación de los BIOS de sus hosts para obtener detalles sobre cómo habilitar HV.

Si el hardware del servidor de ESXi no es compatible con HV, cambie a un hardware que use procesadores que admitan Fault Tolerance.

No hay disponibles hosts compatibles para una máquina virtual secundaria

Si enciende una máquina virtual con Fault Tolerance habilitado y no hay hosts compatibles disponibles para su máquina virtual secundaria, puede que reciba un mensaje de error.

Problema

Podría encontrar el siguiente mensaje de error:

```
Secondary VM could not be powered on as there are no compatible hosts that can accommodate it.
```

Causa

Esto podría deberse a una variedad de razones, como que no hay otros hosts en el clúster, no hay otros hosts con HV habilitado, la virtualización de MMU de hardware no es compatible en las CPU del host, no se puede acceder a almacenes de datos, no hay capacidad disponibles o los hosts están en modo de mantenimiento.

Solución

Si no hay suficientes hosts, agregue más al clúster. Si hay hosts en el clúster, asegúrese de que sean compatibles con HV y que HV esté habilitado. El proceso para habilitar HV es diferente según los BIOS. Consulte la documentación de los BIOS de sus hosts para obtener detalles sobre cómo habilitar HV. Compruebe que los hosts tengan suficiente capacidad y que no estén en modo de mantenimiento.

Una máquina virtual secundaria en un host sobrecomprometido degrada el rendimiento de la máquina virtual principal

Si una máquina virtual principal parece estarse ejecutando lentamente, aunque su host está ligeramente cargado y conserva el tiempo de inactividad de CPU, compruebe el host donde se está ejecutando la máquina virtual secundaria para ver si tiene carga excesiva.

Problema

Cuando una máquina virtual secundaria se encuentra en un host que tiene carga excesiva, esta máquina virtual puede afectar el rendimiento de la máquina virtual principal.

Causa

Es posible que una máquina virtual secundaria que se ejecuta en un host que está sobrecomprometido (por ejemplo, con sus recursos de CPU) no reciba la misma cantidad de recursos que la máquina virtual principal. Cuando ocurre esto, la máquina virtual principal debe desacelerarse para permitir que la máquina virtual secundaria siga el ritmo, lo que reduce eficazmente la velocidad de ejecución a la velocidad menor de la máquina virtual secundaria.

Solución

Si la máquina virtual secundaria está en un host sobrecomprometido, puede mover la máquina virtual a otra ubicación sin problemas de contención de recursos. O más específicamente, haga lo siguiente:

- Para contención de redes de FT, use tecnología vMotion para mover la máquina virtual secundaria a un host con menos máquina virtual de FT que compiten en la red de FT. Compruebe que la calidad del acceso del almacenamiento a la máquina virtual no sea asimétrica.
- En el caso de problemas de contención de almacenamiento, desactive FT y vuelva a activarlo. Cuando recree la máquina virtual secundaria, cambie el almacén de datos de esta a una ubicación con menos contención de recursos y mejor potencial de rendimiento.
- Para resolver un problema de recursos de la CPU, configure una reserva explícita de CPU para la máquina virtual principal con un valor en MHz suficiente para que ejecute su carga de trabajo en el nivel de rendimiento deseado. Esta reserva se aplica tanto a las máquinas virtuales principales como secundarias, lo que asegura que ambas máquinas virtuales puedan ejecutarse a una velocidad especificada. Para obtener instrucciones para configurar esta reserva, vea los gráficos de rendimiento de la máquina virtual (antes de que se habilitara Fault Tolerance) para ver cuántos recursos de CPU utilizó en condiciones normales.

Se observa una mayor latencia de red en máquinas virtuales con FT

Si la red con FT no está configurada de forma óptima, puede que se experimenten problemas de latencia con la máquina virtual con FT.

Problema

Es posible que las máquinas virtuales con FT experimenten un incremento variable en la latencia de paquetes (del orden de milisegundos). Las aplicaciones que exigen muy baja latencia o vibración de paquetes de red (por ejemplo, ciertas aplicaciones en tiempo real) podrían experimentar una degradación en el rendimiento.

Causa

Algo que aumenta la latencia de red es una sobrecarga esperada para Fault Tolerance, pero se pueden agregar ciertos factores a esta latencia. Por ejemplo, si la red de FT está en un vínculo de latencia particularmente alta, esta latencia se pasa a las aplicaciones. Igualmente, si la red con FT tiene un ancho de banda insuficiente (menos de 10 Gbps), podría producirse una mayor latencia.

Solución

Compruebe que la red con FT tenga suficiente ancho de banda (10 Gbps o más) y use un vínculo de latencia baja entre la máquina virtual principal y la secundaria. Estas precauciones no eliminan la latencia de red, pero minimizan su posible impacto.

Algunos hosts están sobrecargados con máquinas virtuales con FT

Podría encontrar problemas de rendimiento si los hosts del clúster tienen una distribución desequilibrada de las máquinas virtuales con FT.

Problema

Algunos hosts en el clúster podrían quedar sobrecargados con máquinas virtuales con FT, mientras que puede que otros tengan recursos sin utilizar.

Causa

vSphere DRS no equilibra la carga de máquinas virtuales con FT (a menos que estén usando FT heredado). Esta limitación podría dar como resultado un clúster donde los hosts están distribuidos de forma dispareja con máquinas virtuales con FT.

Solución

Vuelva a equilibrar manualmente las máquinas virtuales con FT en el clúster utilizando vSphere vMotion. Generalmente, mientras menos máquinas virtuales con FT hay en el host, mejor rendimiento tienen, debido a la reducción de contención para recursos de ancho de banda de red de FT y de CPU.

Perder acceso al almacén de datos de metadatos con FT

El acceso al almacén de datos de metadatos con Fault Tolerance es esencial para el funcionamiento adecuado de una máquina virtual con FT. La pérdida de este acceso puede provocar una variedad de problemas.

Problema

Estos problemas incluyen lo siguiente:

- FT puede finalizar de forma inesperada.

- Si tanto la máquina virtual principal como la secundaria no pueden acceder al almacén de datos de metadatos, podría producirse un error inesperado de las máquina virtual. Por lo general, también debe haber un error no relacionado que finaliza FT cuando ambas máquinas virtuales pierden el acceso al almacén de datos de metadatos con FT. vSphere HA intenta después reiniciar la máquina virtual principal en un host con acceso al almacén de datos de metadatos.
- vCenter Server podría dejar de reconocer la máquina virtual como máquina virtual con FT. Este error de reconocimiento puede permitir operaciones no admitidas, como que la toma de instantáneas se realice en la máquina virtual y provoque un comportamiento problemático.

Causa

La falta de acceso al almacén de datos de metadatos con Fault Tolerance puede producir resultados no deseados de la lista anterior.

Solución

En el momento de planificar su implementación de FT, ponga el almacén de datos de metadatos en almacenamiento de alta disponibilidad. Mientras FT esté ejecutándose, si ve que se pierde el acceso al almacén de datos de metadatos en la máquina virtual principal o la máquina virtual secundaria, solucione cuanto antes el problema de almacenamiento antes de que la pérdida de acceso provoque uno de los problemas anteriores. Si vCenter Server deja de reconocer una máquina virtual como una máquina virtual con FT, no realice operaciones que no se admitan en la máquina virtual. Restaure el acceso al almacén de datos de metadatos. Después de que se restaure el acceso para las máquinas virtuales con FT y haya concluido el período de actualización, las máquinas virtuales quedan reconocibles.

Error al encender vSphere FT para una máquina virtual encendida

Si intenta activar vSphere Fault Tolerance para una máquina virtual encendida, esta operación puede generar errores.

Problema

Cuando seleccione **Turn On Fault Tolerance** (Habilitar Fault Tolerance) para una máquina virtual encendida, la operación genera errores y se muestra un mensaje `Unknown error` (Error desconocido).

Causa

Esta operación puede presentar error si el host en el cual se está ejecutando la máquina virtual no tiene suficientes recursos de memoria para proporcionar protección de Fault Tolerance. vSphere Fault Tolerance intenta automáticamente de asignar una reserva de memoria completa en el host para la máquina virtual. Se requiere memoria de sobrecarga para máquina virtual con

Fault Tolerance y a veces se puede expandir a 1 a 2 GB. Si la máquina virtual encendida está ejecutándose en un host que no posee suficientes recursos de memoria para admitir la reserva completa más la memoria de sobrecarga, se produce error al intentar activar Fault Tolerance. Posteriormente, se arroja el mensaje `Unknown error` (Error desconocido).

Solución

Seleccione entre estas soluciones:

- Libere recursos de memoria en el host para admitir la reserva de memoria de la máquina virtual y la sobrecarga adicional.
- Mueva la máquina virtual a un host con amplios recursos de memoria libre y vuelva a intentarlo.

vSphere DRS no coloca ni evacúa máquinas virtuales con FT

Las máquinas virtuales con FT en un clúster que está habilitado con vSphere DRS no funcionan correctamente si Enhanced vMotion Compatibility (EVC) está deshabilitado actualmente.

Problema

Debido a que EVC es un requisito previo para usar DRS con máquina virtual con FT, DRS no las coloca ni evacúa si EVC se ha deshabilitado (incluso si se vuelve a activar posteriormente).

Causa

Cuando EVC está deshabilitado en un clúster de DRS, es posible agregar un reemplazo por máquina virtual que deshabilita DRS en una máquina virtual con FT. Aunque EVC se vuelva a habilitar posteriormente, esta anulación no se cancela.

Solución

Si DRS no coloca o evacúa máquinas virtuales con FT en el clúster, busque reemplazos por máquinas virtuales que están deshabilitando DRS. Si encuentra una, elimine la anulación que está deshabilitando DRS.

Nota Para obtener más información sobre cómo editar o eliminar anulaciones de máquinas virtuales, consulte *vSphere Administración de recursos*.

Una máquina virtual con Fault Tolerance realiza conmutación por error

Una máquina virtual principal o secundaria puede realizar conmutación por error aunque su host ESXi no haya generado errores. En dichos casos, la ejecución de la máquina virtual no se interrumpe, pero la redundancia se pierde temporalmente. Para evitar este tipo de conmutación por error, esté consciente de algunas de las situaciones en las que se pueden producir y tome las medidas para evitarlas.

Error parcial de hardware relacionado con almacenamiento

Este problema puede surgir cuando el acceso al almacenamiento sea lento o está caído para uno de los hosts. Cuando ocurre esto, hay muchos errores de almacenamiento que se indican en el registro de VMkernel. Para resolver este problema, debe solucionar aquellos relacionados con el almacenamiento.

Error parcial de hardware relacionado con la red

Si la NIC de registro no está funcionando o las conexiones a otros hosts a través de esa NIC están caídas, esto puede activar la conmutación por error de una máquina virtual con Fault Tolerance, de manera que puede restablecerse la redundancia. Con el fin de evitar este problema, dedique una NIC separada para cada vMotion y tráfico de registro de FT, y realice migraciones de vMotion solo cuando las máquinas virtuales estén menos activas.

Ancho de banda insuficiente en la red de NIC de registro

Esto puede ocurrir debido a que hay demasiadas máquinas virtuales con Fault Tolerance en un host. Para solucionar este problema, distribuya de forma más amplia pares de máquinas virtuales con Fault Tolerance entre diferentes hosts.

Use una red de registro de 10 Gbit para FT y verifique que la red tenga baja latencia.

Errores de vMotion debido al nivel de actividad de la máquina virtual

Si hay error en la migración por parte de vMotion de una máquina virtual con Fault Tolerance, es posible que la máquina virtual pueda necesitar conmutación por error. Generalmente, esto ocurre cuando la máquina virtual está demasiado activa para que se realice la migración solo con una interrupción mínima de la actividad. Para evitar este problema, realice migraciones de vMotion únicamente cuando las máquinas virtuales están menos activas.

Demasiada actividad en volumen VMFS pueden conducir a conmutaciones por error de la máquina virtual

Cuando se producen varias operaciones de bloqueo del sistema de archivos, encendidos de máquinas virtuales, apagados de máquinas virtuales o migraciones de vMotion en un solo volumen VMFS, esto puede activar la conmutación por error de máquinas virtuales con Fault Tolerance. Un síntoma de que esto podría estar pasando es recibir muchas advertencias sobre reservas de SCSI en el registro de VMkernel. Para solucionar este problema, reduzca la cantidad de operaciones del sistema de archivos o asegúrese de que la máquina virtual con Fault Tolerance esté en un volumen VMFS que no tenga demasiadas otras máquinas virtuales que regularmente se estén encendiendo, apagando o migrando mediante el uso de vMotion.

Falta de espacio del sistema de archivos evita el inicio de la máquina virtual secundaria

Compruebe si sus sistemas de archivos /(root) o /vmfs/*datasource* tienen o no espacio disponible. Estos sistemas de archivos pueden llenarse por varias razones, y si falta espacio no podrá iniciar una nueva máquina virtual secundaria.

Solucionar problemas de dispositivos de acceso directo a USB

La información sobre el comportamiento de la característica puede ayudar a solucionar o impedir posibles problemas cuando los dispositivos USB están conectados a una máquina virtual.

Mensaje de error cuando intenta migrar una máquina virtual con dispositivos USB conectados

La migración con vMotion no puede continuar y emite un mensaje de error confuso cuando conecta varios dispositivos USB desde un host ESXi a una máquina virtual y uno o más dispositivos no están habilitados para vMotion.

Problema

El asistente Migrate Virtual Machine (Migrar máquina virtual) ejecuta una comprobación de compatibilidad antes de que se inicie una operación de migración. Si se detectan dispositivos USB no compatibles, se produce error en la comprobación de compatibilidad y aparece un mensaje de error similar al siguiente: `Currently connected device 'USB 1' uses backing 'path:1/7/1', which is not accessible`.

Causa

Para aprobar correctamente las comprobaciones de compatibilidad de vMotion, debe habilitar todos los dispositivos USB que están conectados a la máquina virtual desde un host para vMotion. Si uno o más dispositivos no están habilitados para vMotion, habrá error en la migración.

Solución

1. Asegúrese de que los dispositivos no estén en el proceso de transferencia de datos antes de eliminarlos.
2. Vuelva a agregar y habilitar vMotion para cada dispositivo USB afectado.

No es posible copiar datos desde un host ESXi a un dispositivo USB que está conectado al host

Puede conectar un dispositivo USB a un host ESXi y copiar datos al dispositivo desde el host. Por ejemplo, puede que desee recopilar el paquete de vm-support desde el host después de que el host pierde conectividad de red. Para realizar esta tarea, debe detener el árbitro USB.

Problema

Si el árbitro USB se va a utilizar para acceso directo a USB desde un host ESXi a una máquina virtual, el dispositivo USB aparece en `lsusb`, pero no monta correctamente.

Causa

Este problema ocurre debido a que el dispositivo USB que no puede arrancar está reservado para la máquina virtual de forma predeterminada. No aparece en el sistema de archivos del host, aunque `lsusb` puede ver el dispositivo.

Solución

1 Detenga el servicio `usbarbitrator`:`/etc/init.d/usbarbitrator stop`

2 Desconecte físicamente el dispositivo USB y vuelva a conectarlo.

   De manera predeterminada, la ubicación del dispositivo es `/vmfs/devices/disks/mpx.vmhbaXX:C0:T0:L0`.

3 Después de volver a conectar el dispositivo, reinicie el servicio `usbarbitrator`:`/etc/init.d/usbarbitrator start`

4 Reinicie `hostd` y cualquier máquina virtual en ejecución para restaurar el acceso a los dispositivos de acceso directo en la máquina virtual.

Pasos siguientes

Vuelva a conectar los dispositivos USB a la máquina virtual.

Recuperar máquinas virtuales huérfanas

Las máquinas virtuales aparecen con `(orphaned)` anexado a sus nombres.

Problema

En casos raros, las máquinas virtuales que se encuentran en un host ESXi que administra vCenter Server podrían quedar huérfanas. Dichas máquinas virtuales existen en la base de datos de vCenter Server, pero el host ESXi ya no las reconoce.

Causa

Las máquinas virtuales pueden quedar huérfanas si una conmutación por error no se realiza correctamente o cuando la máquina virtual no está registrada directamente en el host. Si se produce esta situación, mueva la máquina virtual a otro host en el centro de datos en el cual están almacenados los archivos de la máquina virtual.

Solución

1 Determine el almacén de datos donde está ubicado el archivo de configuración (`.vmx`) de la máquina virtual.

   a Seleccione la máquina virtual en el inventario de vSphere Web Client y haga clic en la pestaña **Almacenes de datos**.

      Aparecen el o los almacenes de datos donde están almacenados los archivos de la máquina virtual.

   b Si aparece más de un almacén de datos, seleccione cada almacén y haga clic en el icono del explorador de archivos para ver el archivo `.vmx`.

   c Compruebe la ubicación del archivo `.vmx`.

2 Vuelva a la máquina virtual en vSphere Web Client, haga clic con el botón derecho en ella y seleccione **Todas las acciones de infraestructura virtual > Quitar del inventario**.

3 Haga clic en **Sí** para confirmar la eliminación de la máquina virtual.

4 Vuelva a registrar la máquina virtual en vCenter Server.

   a Haga clic con el botón derecho en el almacén de datos donde está ubicado el archivo de la máquina virtual y seleccione **Registrar máquina virtual**.

   b Desplácese hasta el archivo `.vmx` y haga clic en **Aceptar**.

   c Seleccione la ubicación para la máquina virtual y haga clic en **Siguiente**.

   d Seleccione en el host en el cual se ejecutará la máquina virtual y haga clic en **Siguiente**.

   e Haga clic en **Finalizar**.

La máquina virtual no se enciende después de la clonación o implementación desde una plantilla

Las máquinas virtuales no se encienden después de que concluye la clonación o realiza implementación a partir de un flujo de trabajo de plantilla en vSphere Web Client.

Problema

Cuando clona o implementa una máquina virtual a partir de una plantilla, es posible que no pueda encender la máquina después de la creación.

Causa

El tamaño del archivo de intercambio no se reserva cuando se crean los discos de la máquina virtual.

Solución

- Reduzca el tamaño del archivo de intercambio que se requiere para la máquina virtual. Puede hacerlo aumentando la reserva de memoria de la máquina virtual.
  a Haga clic con el botón derecho en la máquina virtual y seleccione **Editar configuración**.
  b Seleccione **Hardware virtual** y haga clic en **Memoria**.
  c Use el menú desplegable Reserva para aumentar la cantidad de memoria asignada a la máquina virtual.
  d Haga clic en **Aceptar**.
- Como alternativa, puede incrementar la cantidad de espacio disponible para el archivo de intercambio sacando otros discos de la máquina virtual del almacén de datos que se utiliza para el archivo de intercambio.
  a Desplácese hasta el almacén de datos en el navegador de objetos de vSphere Web Client.
  b Seleccione la pestaña **Máquinas virtuales**.
  c Para mover cada máquina virtual, haga clic con el botón derecho en la máquina virtual y seleccione **Migrar**.
  d Seleccione **Cambiar solo almacenamiento**.
  e Siga los pasos del asistente **Migrar máquina virtual**.
- También puede aumentar la cantidad de espacio disponible para el archivo de intercambio cambiando la ubicación de este archivo en un almacén de datos con adecuado espacio.
  a Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
  b Seleccione la pestaña **Configurar**.
  c En Máquinas virtuales, seleccione **Ubicación del archivo de intercambio**.
  d Haga clic en **Editar**.

  Nota Si el host forma parte de un clúster que especifica que los archivos de intercambio de la máquina virtual se almacenen en el mismo directorio que la máquina virtual, no podrá hacer clic en **Editar**. Debe usar el cuadro de diálogo Configuración de clúster para cambiar la directiva de ubicación del archivo de intercambio para el clúster.

  e Seleccione **Usar un almacén de datos específico** y seleccione un almacén de datos de la lista.
  f Haga clic en **Aceptar**.

Solucionar problemas de los hosts

3

Los temas de solución de problemas de hosts ofrecen soluciones a posible problemas que se podrían encontrar al usar vCenter Server y hosts ESXi.

Este capítulo incluye los siguientes temas:

Solucionar problemas con estados del host de vSphere HA

vCenter Server informa acerca de los estados del host vSphere HA que indican una condición de error en el host. Dichos errores pueden impedir que vSphere HA proteja completamente las máquinas virtuales en el host y pueden dificultar la capacidad de vSphere HA de reiniciar máquinas virtuales tras un error. Los errores pueden producirse cuando vSphere HA se configura o se anula su configuración en un host o, en casos más raros, durante el funcionamiento normal. Cuando ocurre esto, debe determinar cómo resolver el error, de manera que vSphere HA quede totalmente operativo.

El agente de vSphere HA está en el estado Agente no accesible

El agente de vSphere HA en un host está en el estado Agente inalcanzable durante un minuto o más. Puede que se requiera intervención del usuario para resolver esta situación.

Problema

vSphere HA informa que un agente está en el estado Agente no accesible cuando el host principal o vCenter Server no puede contactar al agente para el host. En consecuencia, vSphere HA no puede supervisar las máquinas virtuales en el host y es posible que no las reinicie después de un error.

Causa

Un agente de vSphere HA puede estar en el estado Agente inaccesible por varios motivos. Generalmente, esta condición indica que un problema de red está impidiendo que vCenter Server o el host primario se pongan en contacto con el agente en el host, o que todos los hosts del clúster presentan un error. Si bien es poco probable, esta condición también puede indicar que vSphere HA se deshabilitó y se volvió a habilitar en el clúster a la vez que vCenter Server no se pudo comunicar con el agente de vSphere HA en el host, o bien que se produjo un error en el agente del host ESXi en el host y el proceso de Watchdog no pudo reiniciarlo. En cualquiera de estos casos, no se activa el evento de conmutación por error si el host entra en estado No accesible.

Solución

Determine si vCenter Server está informando de que el host no está respondiendo. Si es así, existe un problema de redes, un error en el agente del host ESXi o un error de clúster total. Después de que se resuelva el problema, vSphere HA debe funcionar correctamente. Si no es así, vuelva a configurar vSphere HA en el host. De manera similar, si vCenter Server informa que los hosts están respondiendo, pero el estado de un host es Agente inalcanzable, vuelva a configurar vSphere HA en ese host.

vSphere HA Agent is in the Uninitialized State

The vSphere HA agent on a host is in the Uninitialized state for a minute or more. User intervention might be required to resolve this situation.

Problema

vSphere HA reports that an agent is in the Uninitialized state when the agent for the host is unable to enter the run state and become the primary host or to connect to the primary host. Consequently, vSphere HA is not able to monitor the virtual machines on the host and might not restart them after a failure.

Causa

A vSphere HA agent can be in the Uninitialized state for one or more reasons. This condition most often indicates that the host does not have access to any datastores. Less frequently, this condition indicates that the host does not have access to its local datastore on which vSphere HA caches state information, the agent on the host is inaccessible, or the vSphere HA agent is unable to open required firewall ports. It is also possible that the ESXi host agent has stopped.

Solución

Search the list of the host's events for recent occurrences of the event `vSphere HA Agent for the host has an error`. This event indicates the reason for the host being in the uninitialized state. If the condition exists because of a datastore problem, resolve whatever is preventing the host from accessing the affected datastores. If the ESXi host agent has stopped, you must restart it. After the problem has been resolved, if the agent does not return to an operational state, reconfigure vSphere HA on the host.

Nota If the condition exists because of a firewall problem, check if there is another service on the host that is using port 8182. If so, shut down that service, and reconfigure vSphere HA.

vSphere HA Agent is in the Initialization Error State

The vSphere HA agent on a host is in the Initialization Error state for a minute or more. User intervention is required to resolve this situation.

Problema

vSphere HA reports that an agent is in the Initialization Error state when the last attempt to configure vSphere HA for the host failed. vSphere HA does not monitor the virtual machines on such a host and might not restart them after a failure.

Causa

This condition most often indicates that vCenter Server was unable to connect to the host while the vSphere HA agent was being installed or configured on the host. This condition might also indicate that the installation and configuration completed, but the agent did not become a primary host or a secondary host within a timeout period. Less frequently, the condition is an indication that there is insufficient disk space on the host's local datastore to install the agent, or that there are insufficient unreserved memory resources on the host for the agent resource pool. Finally, for ESXi 5.x hosts, the configuration fails if a previous installation of another component required a host reboot, but the reboot has not yet occurred.

Solución

When a Configure HA task fails, a reason for the failure is reported.

Reason for Failure	Action
Host communication errors	Resolve any communication problems with the host and retry the configuration operation.
Timeout errors	Possible causes include that the host crashed during the configuration task, the agent failed to start after being installed, or the agent was unable to initialize itself after starting up. Verify that vCenter Server is able to communicate with the host. If so, see El agente de vSphere HA está en el estado Agente no accesible or vSphere HA Agent is in the Uninitialized State for possible solutions.

Reason for Failure	Action
Lack of resources	Free up approximately 75MB of disk space. If the failure is due to insufficient unreserved memory, free up memory on the host by either relocating virtual machines to another host or reducing their reservations. In either case, retry the vSphere HA configuration task after resolving the problem.
Reboot pending	If an installation for a 5.0 or later host fails because a reboot is pending, reboot the host and retry the vSphere HA configuration task.

vSphere HA Agent is in the Uninitialization Error State

The vSphere HA agent on a host is in the Uninitialization Error state. User intervention is required to resolve this situation.

Problema

vSphere HA reports that an agent is in the Uninitialization Error state when vCenter Server is unable to unconfigure the agent on the host during the Unconfigure HA task. An agent left in this state can interfere with the operation of the cluster. For example, the agent on the host might elect itself as primary host and lock a datastore. Locking a datastore prevents the valid cluster primary host from managing the virtual machines with configuration files on that datastore.

Causa

This condition usually indicates that vCenter Server lost the connection to the host while the agent was being unconfigured.

Solución

Add the host back to vCenter Server (version 5.0 or later). The host can be added as a stand-alone host or added to any cluster.

vSphere HA Agent is in the Host Failed State

The vSphere HA agent on a host is in the Host Failed state. User intervention is required to resolve the situation.

Problema

Usually, such reports indicate that a host has actually failed, but failure reports can sometimes be incorrect. A failed host reduces the available capacity in the cluster and, in the case of an incorrect report, prevents vSphere HA from protecting the virtual machines running on the host.

Causa

This host state is reported when the vSphere HA primary host to which vCenter Server is connected is unable to communicate with the host and with the heartbeat datastores that are in use for the host. Any storage failure that makes the datastores inaccessible to hosts can cause this condition if accompanied by a network failure.

Solución

Check for the noted failure conditions and resolve any that are found.

El agente de vSphere HA está en el estado Con partición de red

El agente de vSphere HA en un host está en el estado Con partición de red. Puede que se requiera intervención del usuario para resolver esta situación.

Problema

Aunque la supervisión de las máquinas virtuales que se ejecutan en el host sigue estando a cargo de los hosts principales que son responsables de ellas, se ve afectada la capacidad de vSphere HA para reiniciar las máquinas virtuales tras un error. En primer lugar, cada host principal tiene acceso a un subconjunto de los hosts, por lo que hay disponible menos capacidad de conmutación por error para cada host. En segundo lugar, es posible que vSphere HA no pueda reiniciar una máquina virtual secundaria FT tras un error (consulte Primary VM Remains in the Need Secondary State).

Causa

Se informa que un host está particionado si se cumplen las siguientes condiciones:

- El host principal de vSphere HA al cual está conectado vCenter Server no puede comunicarse con el host mediante la red de administración (o VMware vSAN™), pero puede comunicarse con ese host mediante los almacenes de datos de latidos que se seleccionaron para él.
- El host no está aislado.

Una partición de red puede producirse por varios motivos, como un etiquetado incorrecto de VLAN, el error de una NIC o conmutadores físicos, la configuración de un clúster con algunos hosts que solo usan IPv4 y otros que únicamente utilizan IPv6, o bien, debido a que las redes de administración para algunos hosts se movieron a un conmutador virtual diferente sin colocar primero el host en modo de mantenimiento.

Solución

Resuelva el problema de redes que evita que los hosts se comuniquen usando las redes de administración.

El agente de vSphere HA está en el estado Aislado de la red

El agente de vSphere HA en un host está en el estado Aislado de la red. Se requiere la intervención del usuario para resolver esta situación.

Problema

Cuando un host está en el estado de aislado de la red, hay dos cosas que se deben considerar: el host aislado y el agente de vSphere HA que tiene el rol principal.

- En el host aislado, el agente de vSphere HA aplica la respuesta configurada de aislamiento a las máquinas virtuales en ejecución, lo que determina si deben desactivarse o apagarse. Esto lo hace después de comprobar si el agente principal puede asumir la responsabilidad para cada máquina virtual (bloqueando el almacén de datos de inicio de la máquina virtual). Si no, el agente aplaza la aplicación de la respuesta de aislamiento para la máquina virtual y vuelve a comprobar el estado del almacén de datos después de un breve retraso.
- Si el agente principal de vSphere HA puede acceder a uno o más almacenes de datos, supervisa las máquinas virtuales que se estaban ejecutando en el host cuando quedó aislado e intenta reiniciar cualquiera de las que estaban apagadas o desconectadas.

Causa

Un host está aislado de la red si se cumplen estas dos condiciones:

- Las direcciones de aislamiento se han configurado y el host no puede les puede hacer ping.
- El agente de vSphere HA en el host no puede acceder a alguno de los agentes que se ejecutan en otros hosts del clúster.

Nota Si su clúster de vSphere HA tiene vSAN habilitado, se determina que un host está aislado si no puede comunicarse con los otros agentes de vSphere HA en el clúster y no logra llegar a las direcciones de aislamiento configuradas. Aunque los agentes de vSphere HA usan la red de vSAN para la comunicación entre agentes, la dirección de aislamiento predeterminada sigue siendo la puerta de enlace del host. Por lo tanto, en la configuración predeterminada, debe haber errores en ambas redes para que un host se declare aislado.

Solución

Resuelva el problema de redes que impide que el host haga ping a sus direcciones de red y se comunique con otros hosts.

Se agotó el tiempo de espera de la configuración de vSphere HA en hosts

La configuración de un clúster de vSphere HA podría agotar el tiempo de espera en alguno de los hosts que se le agregan.

Problema

Cuando se habilita vSphere HA en un clúster existente con gran cantidad de hosts y máquinas virtuales, podría haber error en la configuración de vSphere HA en algunos de los hosts.

Causa

El error es resultado de un tiempo de espera que se produce antes de que concluya la instalación de vSphere HA en el o los hosts.

Solución

Configure la opción avanzada de vCenter Server config.vpxd.das.electionWaitTimeSec en value=240. Una vez hecho este cambio, no se producen tiempos de espera.

Solución de problemas de vSphere Auto Deploy

Los temas de solución de problemas de vSphere Auto Deploy ofrecen soluciones para situaciones en las que el aprovisionamiento de hosts con vSphere Auto Deploy no funciona según lo esperado.

Error de tiempo de espera de TFTP de vSphere Auto Deploy durante el arranque

Se muestra el mensaje de error de tiempo de espera de TFTP en el arranque de un host aprovisionado con vSphere Auto Deploy. El texto del mensaje depende del BIOS.

Problema

Se muestra el mensaje de error de tiempo de espera de TFTP en el arranque de un host aprovisionado con vSphere Auto Deploy. El texto del mensaje depende del BIOS.

Causa

El servidor TFTP está caído o no está accesible.

Solución

- Asegúrese de que el servicio TFTP esté en ejecución y accesible para el host que está intentando arrancar.
- Para ver los registros de diagnóstico y obtener más información sobre el error presente, consulte la documentación del servicio TFTP.

El host vSphere Auto Deploy arranca con una configuración incorrecta

Un host está arrancando con una imagen, perfil de host o ubicación de carpeta de ESXi diferentes de los especificados en las reglas.

Problema

Un host está arrancando con un perfil de imagen o configuración de ESXi diferentes a los que especifican las reglas. Por ejemplo, puede cambiar las reglas para asignar un perfil de imagen diferente, pero el host sigue usando el perfil de imagen antiguo.

Causa

Una vez que se agrega el host a un sistema vCenter Server, el sistema vCenter Server determina la configuración de arranque. El sistema vCenter Server asociará un perfil de imagen, un perfil de host o la ubicación de carpeta con el host.

Solución

- Use los cmdlets de vSphere PowerCLI `Test-DeployRuleSetCompliance` y `Repair-DeployRuleSetCompliance` para reevaluar las reglas y asociar el perfil de imagen, el perfil de host o la ubicación de carpeta correctos con el host.

No se redirige el host al servidor vSphere Auto Deploy

Durante un arranque, un host que se desea aprovisionar con vSphere Auto Deploy carga iPXE. El host no se redirige al servidor vSphere Auto Deploy.

Problema

Durante un arranque, un host que se desea aprovisionar con vSphere Auto Deploy carga iPXE. El host no se redirige al servidor vSphere Auto Deploy.

Causa

El archivo `tramp` que se incluye en el archivo ZIP TFTP tiene la dirección IP incorrecta para el servidor vSphere Auto Deploy.

Solución

- Corrija la dirección IP del servidor vSphere Auto Deploy en el archivo `tramp`, según se explica en la documentación *Instalación y configuración de vSphere*.

Mensaje de advertencia de paquete cuando se asigna un perfil de imagen al host vSphere Auto Deploy

Cuando se ejecuta un cmdlet de vSphere PowerCLI para asignar un perfil de imagen que no está preparado para vSphere Auto Deploy, se muestra un mensaje de advertencia.

Problema

Cuando escribe o modifica reglas para asignar un perfil de imagen a uno o más hosts, se produce el siguiente error:

```
Warning: Image Profile <name-here> contains one or more software packages
that are not stateless-ready. You may experience problems when using this
profile with Auto Deploy.
```

Causa

Cada VIB en un perfil de imagen tiene una marca `stateless-ready` para indicar que el VIB se diseñó para usarse con vSphere Auto Deploy. El error se produce al intentar escribir una regla de vSphere Auto Deploy donde se usa un perfil de imagen en el cual uno o más VIB tienen esa marca establecida en FALSE.

Nota Es posible usar sin problemas los hosts aprovisionados con vSphere Auto Deploy que incluyen VIB no preparados para estar sin estado. Sin embargo, un arranque con un perfil de imagen que incluye VIB que no están preparados para estar sin estado se trata como una instalación nueva. Cada vez que se arranca el host, se pierden datos de configuración que se encontrarían disponibles a través de reinicios para hosts aprovisionados con vSphere Auto Deploy.

Solución

1 Utilice cmdlets de vSphere ESXi Image Builder en una sesión de vSphere PowerCLI para ver los VIB en el perfil de imagen.
2 Quite cualquier VIB que no esté preparado para estar sin estado.
3 Vuelva a ejecutar el cmdlet de vSphere Auto Deploy.

El host vSphere Auto Deploy con una unidad flash USB integrada no envía volcados de memoria al disco local

Si el host vSphere Auto Deploy presenta una unidad flash USB integrada y un error produce un volcado de memoria, el volcado se pierde. Configure el sistema de modo que se use ESXi Dump Collector para almacenar volcados de memoria en un host en red.

Problema

Si el host vSphere Auto Deploy presenta una unidad USB flash integrada y se detecta que un error produce un volcado de memoria, el volcado de memoria no se envía al disco local.

Solución

1 Instale ESXi Dump Collector en el sistema de su elección.

   ESXi Dump Collector se incluye con el instalador de vCenter Server.

2 Use ESXCLI para configurar el host de modo que use ESXi Dump Collector.

```
esxcli conn_options system coredump network set IP-addr,port
esxcli system coredump network set -e true
```

3 Utilice ESXCLI para deshabilitar particiones de volcado de memoria locales.

```
esxcli conn_options system coredump partition set -e false
```

El host vSphere Auto Deploy se reinicia después de cinco minutos

El host vSphere Auto Deploy arranca y muestra información de iPXE, pero se reinicia tras cinco minutos.

Problema

Un host que se aprovisionará con vSphere Auto Deploy arranca desde iPXE y muestra información de iPXE en la consola. Sin embargo, tras cinco minutos, el host muestra el siguiente mensaje a la consola y se reinicia.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

El host también podría mostrar los siguientes detalles:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

Luego, la consola muestra los atributos de las máquinas del host incluido el proveedor, el número de serie, la dirección IP, etc.

Causa

No hay un perfil de imagen actualmente asociado con este host.

Solución

Es posible asignar un perfil de imagen al host. Para ello, ejecute el cmdlet `Apply-EsxImageProfile` o cree la siguiente regla:

1 Ejecute el cmdlet `New-DeployRule` para crear una regla que incluya un patrón que coincida con el host con un perfil de imagen.

2 Ejecute el cmdlet `Add-DeployRule` para agregar la regla a un conjunto de reglas.

3 Ejecute el cmdlet `Test-DeployRuleSetCompliance` y use el resultado de ese cmdlet como entrada para el cmdlet de `Repair-DeployRuleSetCompliance`.

El host vSphere Auto Deploy no puede contactar con el servidor TFTP

El host que se aprovisiona con vSphere Auto Deploy no puede contactar con el servidor TFTP.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host realiza un arranque de red y el servidor DHCP le asigna una dirección DHCP, pero el host no puede contactar con el servidor TFTP.

Causa

El servidor TFTP podría haber dejado de ejecutarse o un firewall podría bloquear el puerto TFTP.

Solución

- Si instaló el servidor TFTP de WinAgents, abra la consola de administración TFTP de TFTP y compruebe que el servicio esté en ejecución. Si el servicio se está ejecutando, compruebe las reglas de entrada del firewall de Windows para asegurarse de que el puerto TFTP no esté bloqueado. Desactive temporalmente el firewall para ver si este es el problema.
- Para todos los otros servidores TFTP, consulte la documentación para procedimientos de depuración.

El host vSphere Auto Deploy no puede recuperar una imagen de ESXi del servidor vSphere Auto Deploy

El host que se aprovisiona con vSphere Auto Deploy se detiene en la pantalla de arranque de iPXE.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el proceso de arranque se detiene en la pantalla de arranque de iPXE y el mensaje de estado indica que el host intenta obtener la imagen de ESXi del servidor vSphere Auto Deploy.

Causa

Es posible que el servicio de vSphere Auto Deploy se haya detenido o que no se pueda acceder al servidor vSphere Auto Deploy.

Solución

1. Inicie sesión en el sistema en el cual instaló el servidor vSphere Auto Deploy.
2. Compruebe que el servidor vSphere Auto Deploy esté en ejecución.
   a. Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas**.
   b. Haga doble clic en **Servicios** para abrir el panel Administración de servicios.
   c. En el campo Servicios, busque el servicio VMware vSphere Auto Deploy Waiter y reinícielo si no está en ejecución.

3 Abra un explorador web, introduzca la siguiente URL y compruebe si es posible acceder al servidor vSphere Auto Deploy.

https://*Auto_Deploy_Server_IP_Address*:*Auto_Deploy_Server_Port*/vmw/rdb

Nota Use esta dirección solo para comprobar si se puede tener acceso al servidor.

4 Si no es posible hacerlo, probablemente hay un problema con el firewall.

   a Intente configurar reglas de entrada de TCP permisivas para el puerto del servidor vSphere Auto Deploy.

   El puerto es 6501 a menos que haya especificado uno diferente durante la instalación.

   b Como último recurso, deshabilite temporalmente el firewall y vuelva a habilitarlo después de que haya verificado si bloqueó el tráfico. No deshabilite el firewall en entornos de producción.

   Para deshabilitar el firewall, ejecute **`netsh firewall set opmode disable`**. Para habilitar el firewall, ejecute **`netsh firewall set opmode enable`**.

El host vSphere Auto Deploy no obtiene una dirección asignada por DHCP

El host que se aprovisiona con vSphere Auto Deploy no recibe una dirección DHCP.

Problema

Cuanto se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host realiza un arranque de red, pero presenta una dirección DHCP asignada. El servidor vSphere Auto Deploy no puede aprovisionar el host con el perfil de imagen.

Causa

Puede que tenga un problema con el servicio DHCP o con la instalación del firewall.

Solución

1 Compruebe que el servicio de servidor DHCP esté ejecutándose en el sistema Windows en el cual el servidor DHCP está instalado para aprovisionar hosts.

   a Haga clic en **Inicio > Configuración > Panel de control > Herramientas administrativas**.

   b Haga doble clic en **Servicios** para abrir el panel Administración de servicios.

   c En el campo Servicios, busque el servicio de servidor DHCP y reinicie el servicio si no está en ejecución.

2 Si el servidor DHCP está en ejecución, vuelva a comprobar el ámbito de DHCP y las reservas de DHCP que configuró para sus hosts de destino.

   Si el ámbito y reservas de DHCP están configurados de forma correcta, lo más probable es que el problema involucre al firewall.

3 Como solución alternativa temporal, apague el firewall para ver si eso resuelve el problema.

   a Abra el símbolo del sistema haciendo clic en **Inicio > Programa > Accesorios > Símbolo del sistema**.

   b Escriba el siguiente comando para apagar temporalmente el firewall. No apague el firewall en un entorno de producción.

   ```
   netsh firewall set opmode disable
   ```

   c Intente aprovisionar el host con vSphere Auto Deploy.

   d Escriba el siguiente comando para volver a encender el firewall.

   ```
   netsh firewall set opmode enable
   ```

4 Instale reglas para permitir tráfico de red DHCP hacia los hosts de destino.

   Consulte la documentación del firewall para ver los detalles del DHCP y del sistema Windows en el cual se ejecuta el servidor DHCP.

El host vSphere Auto Deploy no realiza el arranque de red

El host que se aprovisiona con vSphere Auto Deploy se activa, pero no realiza el arranque de red.

Problema

Cuando se intenta arrancar un host aprovisionado con vSphere Auto Deploy, el host no inicia el proceso de arranque de red.

Causa

No habilitó el host para el arranque de red.

Solución

1 Reinicie el host y siga las instrucciones en pantalla para acceder a la configuración del BIOS.

2 En la configuración del BIOS, habilite el arranque de red en la configuración de dispositivo de arranque.

Recuperarse de daños en la base de datos en el servidor vSphere Auto Deploy

En ciertas situaciones, es posible que experimente un problema con la base de datos de vSphere Auto Deploy. La opción de recuperación más eficaz es reemplazar el archivo de base de datos actual con la copia de seguridad más reciente.

Problema

Al usar vSphere Auto Deploy para aprovisionar los hosts ESXi del entorno, es posible que experimente un problema con la base de datos de vSphere Auto Deploy.

Importante Se trata de un problema poco frecuente. Siga todas las demás estrategias de solución de problemas de vSphere Auto Deploy antes de reemplazar el archivo de base de datos actual. Se perderán las reglas o las asociaciones que haya creado desde la copia de seguridad que elija.

Causa

Este problema ocurre únicamente en los hosts aprovisionados con vSphere Auto Deploy.

Solución

1 Detenga el servicio del servidor vSphere Auto Deploy.

2 Busque el registro de vSphere Auto Deploy desde la página de vSphere Auto Deploy en vSphere Web Client.

3 Busque el siguiente mensaje en los registros:

   `DatabaseError: database disk image is malformed.`

   Si ve este mensaje, reemplace el archivo de base de datos existente con la copia de seguridad más reciente.

4 Vaya al directorio de datos de vSphere Auto Deploy.

Sistema operativo	Ubicación del archivo
vCenter Server Appliance	`/var/lib/rbd`
Microsoft Windows	`%VMWARE_DATA_DIR%\autodeploy\Data`

   El directorio contiene un archivo denominado `db` y los archivos de copia de seguridad denominados `db`-*yyy*-*mm*-*dd*.

5 Cambie el nombre del archivo `db` actual.

   Si solicita asistencia, es posible que el servicio de soporte de VMware le pida ese archivo.

6 Cambie el nombre de la copia de seguridad más reciente a `db`.

7 Reinicie el servicio del servidor vSphere Auto Deploy.

8 Si el mensaje sigue apareciendo en el registro, repita los pasos para usar la siguiente copia de seguridad más reciente hasta que vSphere Auto Deploy funcione sin mostrar errores de la base de datos.

Error de manipulación de token de autenticación

La creación de una contraseña que no cumple con los requisitos de autenticación del host provoca un error.

Problema

Al crear una contraseña en el host, se muestra el siguiente mensaje de error: `Se produjo un error general del sistema: contraseña: Error de manipulación de token de autenticación`.

Se incluye el siguiente mensaje: `No se pudo establecer la contraseña. Es posible que la contraseña no cumpla los criterios de complejidad establecidos por el sistema.`

Causa

El host comprueba el cumplimiento de la contraseña mediante el complemento de autenticación predeterminado, `pam_passwdqc.so`. Si la contraseña no cumple con las normas, aparece el error.

Solución

Al crear una contraseña, se debe incluir una combinación de cuatro tipo de caracteres: minúsculas, mayúsculas, números y caracteres especiales, como guion o guion bajo.

La contraseña de usuario debe cumplir con los siguientes requisitos de longitud.

- Las contraseñas que contienen caracteres de tres clases, deben tener al menos ocho caracteres en total.
- Las contraseñas que contienen caracteres de las cuatro clases deben tener al menos siete caracteres de longitud.

Nota Un carácter en mayúscula al inicio de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan. Un número al final de una contraseña no se tiene en cuenta en la cantidad de clases de caracteres que se utilizan.

Para obtener más información, consulte la documentación sobre *Seguridad de vSphere*.

Un error de conjunto de reglas de Active Directory provoca error de cumplimiento del perfil de host

La aplicación de un perfil de host que especifica un dominio de Active Directory al cual unirse provoca un error de cumplimiento.

Problema

Cuando aplica un perfil de host que especifica un dominio de Active Directory al cual unirse, pero no habilita el conjunto de reglas **activeDirectoryAll** en la configuración de firewall, se produce un error de cumplimiento. vSphere Web Client muestra el mensaje de error `Errores de cumplimiento del perfil de host: El conjunto de reglas activedirectoryAll no coincide con la especificación`. El error de cumplimiento también se produce cuando aplica un perfil de host para abandonar un dominio de Active Directory, pero no deshabilita el conjunto de reglas **activeDirectoryAll** en el perfil de host.

Causa

Active Directory requiere el conjunto de reglas de firewall **activeDirectoryAll**. Debe habilitar el conjunto de reglas en la configuración del firewall. Si omite esta configuración, el sistema agrega las reglas de firewall necesarias cuando el host se une al dominio, pero habrá incumplimiento del host debido a que las reglas de firewall no coinciden. También habrá no cumplimiento del host si lo elimina del dominio sin deshabilitar el conjunto de reglas de Active Directory.

Solución

1 Desplácese hasta el perfil de host en vSphere Web Client.

   Para buscar un perfil de host, haga clic en **Directivas y perfiles > Perfiles de host** en la página de inicio de vSphere Web Client.

2 Haga clic con el botón derecho en el perfil de host y seleccione **Editar configuración**.

3 Haga clic en **Siguiente**.

4 Seleccione **Seguridad y servicios > Configuración del firewall > Configuración del firewall > Configuración del conjunto de reglas**.

5 Asegúrese de seleccionar la opción **activeDirectoryAll**.

6 En el panel derecho, active la casilla de verificación **Marca que indica que se debe usar conjunto de reglas**.

   Anule la selección de la casilla si el host va a abandonar el dominio.

7 Haga clic en **Siguiente** y luego en **Finalizar** para cambiar el perfil de host.

No se pueden descargar VIB cuando se utiliza el proxy inverso de vCenter Server

No se pueden descargar VIB si vCenter Server utiliza un puerto personalizado para el proxy inverso.

Problema

Si se configura el proxy inverso de vCenter Server para utilizar un puerto personalizado, se produce un error en las descargas de VIB.

Causa

Si vCenter Server utiliza un puerto personalizado para el proxy inverso, el puerto personalizado no se habilita de forma automática en el firewall de ESXi y se produce un error en las descargas de VIB.

Solución

1 Abra una conexión SSH al host e inicie sesión como raíz.

2 (opcional) Enumere las reglas de firewall existentes.

```
esxcli network firewall ruleset list
```

3 (opcional) Realice una copia de seguridad del archivo `/etc/vmware/firewall/service.xml`.

```
cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
```

4 Edite los permisos de acceso del archivo `service.xml` para permitir la escritura. Para ello, ejecute el comando `chmod`.

   - Para permitir la escritura, ejecute `chmod644/etc/vmware/firewall/service.xml`.
   - Para alternar la marca de sticky bit, ejecute `chmod+t /etc/vmware/firewall/service.xml`.

5 Abra el archivo `service.xml` en un editor de texto.

6 Agregue una nueva regla al archivo `service.xml` para habilitar el puerto personalizado en el proxy inverso de vCenter Server.

```
<service id='id_value'>
   <id>vcenterrhttpproxy</id>
   <rule id='0000'>
     <direction>outbound</direction>
     <protocol>tcp</protocol>
     <port type='dst'>custom_reverse_proxy_port</port>
   </rule>
   <enabled>true</enabled>
   <required>false</required>
</service>
```

Donde *id_ value* debe ser un valor único. Por ejemplo, si el último servicio detallado en el archivo `service.xml` tiene el identificador 0040, se debe escribir el número 0041.

7 Revierta los permisos de acceso del archivo `service.xml` al valor predeterminado de solo lectura.

```
chmod 444 /etc/vmware/firewall/service.xml
```

8 Actualice las reglas de firewall para que se apliquen los cambios.

```
esxcli network firewall refresh
```

9 (opcional) Enumere el conjunto de reglas actualizado para confirmar el cambio.

```
 esxcli network firewall ruleset list
```

10 (opcional) Si desea conservar la configuración de firewall después de reiniciar el host ESXi, copie `service.xml` en el almacenamiento persistente y modifique el archivo `local.sh`.

   a Copie el archivo `service.xml` modificado en el almacenamiento persistente (por ejemplo, `/store/`) o en un volumen VMFS (por ejemplo, `/vmfs/volumes/volume/`).

   ```
   cp /etc/vmware/firewall/service.xml location_of_xml_file
   ```

   Es posible almacenar un volumen VMFS en una sola ubicación y copiarlo a varios hosts.

   b Agregue la información del archivo `service.xml` al archivo `local.sh` en el host.

   ```
   cp location_of_xml_file /etc/vmware/firewall
   esxcli network firewall refresh
   ```

   En el ejemplo anterior, *location_of_xml_file* es la ubicación en la que se copió el archivo.

Solucionar problemas de vCenter Server y vSphere Web Client

4

Los temas de solución de problemas de vCenter Server y vSphere Web Client ofrecen soluciones a problemas que podría encontrar al instalar y configurar vCenter Server y vSphere Web Client, incluso vCenter Single Sign-On.

Este capítulo incluye los siguientes temas:

- Solucionar problemas de vCenter Server
- Solucionar problemas de vSphere Web Client
- Solucionar problemas de certificados de host vCenter Server y ESXi

Solucionar problemas de vCenter Server

Estos temas de solución de problemas ofrecen soluciones a problemas que se podrían encontrar al instalar vCenter Server en el sistema operativo Windows o al implementar vCenter Server Appliance en un sistema Linux.

La actualización de vCenter Server genera errores cuando no puede detener el servicio Tomcat

Una actualización de vCenter Server puede generar errores cuando un instalador no puede detener el servicio Tomcat.

Problema

Si el instalador de vCenter Server no puede detener el servicio Tomcat durante una actualización, esta genera errores y muestra un mensaje similar a `Unable to delete VC Tomcat service` (No se puede eliminar servicio Tomcat de VC). Este problema puede producirse incluso si detiene el servicio Tomcat de forma manual antes de la actualización, si es que se bloquean algunos archivos que utiliza el proceso Tomcat.

Solución

1 En el menú **Start** (Inicio) de Windows, seleccione **Settings (Configuración) > Control Panel (Panel de control) > Administrative Tools (Herramientas administrativas) > Services (Servicios)**.

2 Haga clic con el botón derecho en **VMware VirtualCenter Server** y seleccione **Manual**.

3 Haga clic con el botón derecho en **VMware vCenter Management Webservices** y seleccione **Manual**.

4 Reinicie la máquina de vCenter Server antes de la actualización.

   Esto libera cualquier archivo bloqueado que utilice el proceso Tomcat y habilita el instalador de vCenter Server para detener el servicio Tomcat para la actualización.

Solución

Como alternativa, puede reiniciar la máquina de vCenter Server y reiniciar el proceso de actualización, pero seleccione la opción de no sobrescribir los datos de vCenter Server.

Microsoft SQL Database configurado en modo de compatibilidad no admitido provoca errores en la instalación o actualización de vCenter Server

Se produce un error en la instalación de vCenter Server con una base de datos de Microsoft SQL cuando la base de datos está configurada en modo de compatibilidad con una versión no compatible.

Problema

Aparece el siguiente mensaje de error: `El usuario de base de datos ingresado no tiene los permisos necesarios para instalar y configurar vCenter Server con la base de datos seleccionada. Corrija los siguientes errores: %s`

Causa

La versión de la base de datos debe ser compatible para vCenter Server. En el caso de SQL, aunque la base de datos sea de una versión compatible, si se configura para que se ejecute en modo de compatibilidad con una versión no compatible, se produce este error. Por ejemplo, si SQL 2008 está configurada para que ejecute el modo de compatibilidad de SQL 2000, se presenta este error.

Solución

- Asegúrese de que la base de datos de vCenter Server sea de una versión compatible y no esté configurada en el modo de compatibilidad con una versión no compatible. Consulte las matrices de interoperabilidad de productos VMware en http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Solucionar problemas de vSphere Web Client

Los temas de vSphere Web Client ofrecen soluciones a posibles problemas que podría encontrar al usar vSphere Web Client para administrar componentes de vSphere, que incluye vCenter Single Sign-On y vCenter Server.

El sistema de vCenter Server no aparece en el inventario de vSphere Web Client

vSphere Web Client no aparece en los sistemas de vCenter Server que espera ver en el inventario.

Problema

Cuando inicia sesión en vSphere Web Client, el inventario parece estar vacío o el sistema de vCenter Server que espera ver no aparece.

Causa

En vSphere 5.1 y versiones posteriores, se inicia sesión en vSphere Web Client para ver y administrar varias instancias de vCenter Server. Cualquier sistema de vCenter Server en el cual tenga permisos aparece en el inventario, en caso de que el servidor esté registrado en el mismo Component Manager que vSphere Web Client.

Solución

- Inicie sesión en vSphere Web Client como usuario con permisos en el sistema de vCenter Server.

  El sistema de vCenter Server no aparecerá en el inventario si no tiene permisos en él. Por ejemplo, si inicia sesión como usuario administrador de vCenter Single Sign On, es posible que no tenga permisos en algún sistema de vCenter Server.

- Compruebe que el sistema de vCenter Server esté registrado en el mismo Component Manager que vSphere Web Client.

  vSphere Web Client detecta solo sistemas de vCenter Server que están registrados en el mismo Componenent Manager.

No se puede iniciar la consola de máquina virtual

Cuando intenta abrir una consola de máquina virtual desde vSphere Web Client, la consola no se abre.

Problema

Cuando intenta abrir una consola de máquina virtual desde vSphere Web Client, la consola no se abre. Aparece el siguiente mensaje de error:

```
HTTP ERROR 404 Problem accessin /. Reason: Not Found
```

Errores similares a los siguientes aparecen en el archivo `virgo-server.log`:

```
[2012-10-03 18:34:19.170] [ERROR] Thread-40 System.err 2012-10-03
18:34:19.167:WARN:oejuc.AbstractLifeCycle:FAILED org.eclipse.jetty.server.Server@315b0333:
java.net.BindException: Address already in use [2012-10-03 18:34:19.170] [ERROR] Thread-40
System.err java.net.BindException: Address already in use
```

Causa

Otro programa o proceso está usando el puerto 9443, el puerto predeterminado que usa la consola de máquina virtual HTML5.

Solución

- Edite el archivo `webclient.properties` para agregar la línea `html.console.port=port`, donde*port* es el nuevo número de puerto.

  El archivo `webclient.properties` se encuentra en una de las siguientes ubicaciones, según el sistema operativo que haya en la máquina en la cual está instalado vSphere Web Client:

Windows 2008	`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\`
vCenter Server Appliance	`/etc/vmware/vsphere-client/`

Solución de problemas en los filtros de extensión

Los complementos retrasan la visualización de partes de vSphere Web Client.

Problema

Cuando el usuario se desplaza por una vista de vSphere Web Client, el mecanismo de extensibilidad proporciona todas las extensiones de la interfaz de usuario a la vista de extensión específica. De una lista de posibles extensiones que pueden mostrarse, el vSphere Web Client reduce la lista a las extensiones que corresponden al contexto en particular mediante un conjunto de filtros de extensión. Algunos de estos filtros se ejecutan de forma asíncrona y demoran la evaluación de todas las extensiones si se envía una solicitud a un servicio que no responde.

Aparece la siguiente ventana emergente en la esquina inferior derecha de vSphere Web Client

```
No se pudieron mostrar algunos elementos o no se pudo recuperar su información a tiempo.
Póngase en contacto con el administrador para solucionar el problema.
```

Si el elemento emergente está oculto, otro posible problema es que una pestaña se muestre o no en un objeto de inventario que no es relevante.

Causa

Estos mensajes aparecen debido a un tiempo de espera que ahora se aplica al cálculo correspondiente a los diferentes elementos de la interfaz de usuario provenientes de los complementos de vSphere Web Client. Antes de introducir los tiempos de espera, un complemento puede causar que grandes partes de la interfaz de usuario se demoren dos o más minutos. El mensaje emergente aparece cuando una evaluación dura más de 20 segundos.

Solución

Cuando aparece el elemento emergente, el archivo de registro (`vsphere_client_virgo.log`) contiene un error que muestra el filtro para el cual se agotó el tiempo de espera y las extensiones afectadas.

Un ejemplo del archivo `vsphere_client_virgo.log`es el siguiente:

```
2016-06-08T20:29:07.358Z] [ERROR] http-bio-9090-exec-4 70000174
100005 200003
com.vmware.vise.util.logging.LogServiceImpl
Extension
filter timeout: \
vsphere.misbehaving.slowFilter/com.vmware.misbehaving.slowfilter.filters.SlowCustomFilter
could not complete execution in 8000 ms. \
Extensions
[vsphere.core.cluster.manage.slowView/com.vmware.misbehaving.slowportlet.ui:6.5.0;
] processed by the filter will not be loaded.
[2016-06-08T20:29:19.314Z] [ERROR] http-bio-9090-exec-8 70000175
100005 200003 com.vmware.vise.util.logging.LogServiceImpl Extension
filter timeout: \
vsphere.core.objectPropertyFilter/com.vmware.vsphere.client.filters.ObjectPropertyFilter
could not complete execution in 20000 ms. \
Extensions
[vsphere.core.cluster.monitor.slowView/com.vmware.misbehaving.slowportlet.ui:6.5.0;
\
vsphere.core.cluster.monitor.vsanView/com.vmware.vsphere.client.vsanui:6.5.0;
\
vsphere.core.cluster.monitor.drsView/com.vmware.vsphere.client.clusterui:6.5.0;
\
vsphere.core.cluster.monitor.haView/com.vmware.vsphere.client.clusterui:6.5.0;
] processed by the filter will be loaded.
```

El complemento externo a VMware puede identificarse como la posible causa del problema y bloquearse mediante la nueva función de compatibilidad de complementos. Como alternativa, si el problema no es evidente, se pueden deshabilitar todos los complementos secundarios para verificar si el problema persiste.

Solucionar problemas de certificados de host vCenter Server y ESXi

Los certificados se generan automáticamente cuando se instala vCenter Server. Estos certificados predeterminados no cuentan con la firma de una autoridad de certificación (CA) comercial y puede que no proporcionen una seguridad sólida. Puede reemplazar los certificados predeterminados de vCenter Server con certificados firmados por una CA comercial. Cuando se reemplazan certificados de vCenter Server y ESXi, puede que se encuentren errores.

vCenter Server no puede conectarse con hosts administrados

Después de reemplazar certificados predeterminados de vCenter Server y reiniciar el sistema, es posible que vCenter Server no pueda conectarse a hosts administrados.

Problema

vCenter Server no puede conectarse a hosts administrados después de reemplazar certificados del servidor y de que se reinicia el sistema.

Solución

Inicie sesión en el host como usuario raíz y vuelva a conectar al host a vCenter Server.

Parece que un nuevo certificado de vCenter Server no se carga

Después de reemplazar certificados predeterminados de vCenter Server, puede que parezca que los nuevos certificados no se cargan.

Problema

Cuando se instalan nuevos certificados de vCenter Server, es posible que no vea el nuevo certificado.

Causa

No se fuerza el cierre de las conexiones abiertas existentes con vCenter Server y es posible que estas sigan usando el certificado antiguo.

Solución

Para forzar que todas las conexiones usen el certificado nuevo, utilice uno de los siguientes métodos.

- Reinicie la pila de red o las interfaces de red en el servidor.
- Reinicie el servicio de vCenter Server.

No se puede configurar vSphere HA cuando se utilizan certificados SSL personalizados

Después de instalar certificados SSL personalizados, se produce error al intentar habilitar vSphere High Availability (HA).

Problema

Cuando intenta habilitar vSphere HA en un host que tiene instalados certificados SSL personalizados, aparece el siguiente mensaje de error: `vSphere HA cannot be configured on this host because its SSL thumbprint has not been verified.`

Causa

Cuando agrega un host a vCenter Server y vCenter Server ya confía en el certificado SSL del host, `VPX_HOST.EXPECTED_SSL_THUMBPRINT` no se rellena en la base de datos de vCenter Server. vSphere HA obtiene la huella digital SSL del host desde este campo en la base de datos. Sin la huella digital, no puede habilitar vSphere HA.

Solución

1. En vSphere Web Client, desconecte el host que tiene instalados certificados SSL personalizados.

2. Vuelva a conectar el host a vCenter Server.
3. Acepte el certificado SSL del host.
4. Habilite vSphere HA en el host.

Solucionar problemas de disponibilidad

5

Los temas de solución de problemas de disponibilidad ofrecen soluciones a posibles problemas que se podrían encontrar cuando se usan los hosts y almacenes de datos en clústeres de vSphere HA.

Es posible que se reciba un mensaje de error cuando se intenta usar vSphere HA o vSphere FT. Para obtener información sobre estos mensajes de error, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1033634.

Este capítulo incluye los siguientes temas:

Solucionar problemas de control de admisión de vSphere HA

vCenter Server utiliza control de admisión para asegurar que se reserven suficientes recursos en un clúster de vSphere HA para recuperación de máquinas virtuales en caso de error del host.

Si el control de admisión de vSphere HA no funciona adecuadamente, no hay garantía de que todas las máquinas virtuales del clúster puedan reiniciarse después de un error del host.

Clúster rojo debido a recursos de conmutación por error insuficientes

Cuando utiliza la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), los clústeres de vSphere HA podrían quedar invalidados (rojos) debido a insuficientes recursos de conmutación por error.

Problema

Si selecciona la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) y surgen ciertos problemas, el clúster se vuelve de color rojo.

Causa

Este problema puede surgir cuando los hosts del clúster están desconectados, en modo de mantenimiento, no responden o tienen un error de vSphere HA. Los hosts en modo desconectado y de mantenimiento suelen deberse a una acción provocada por el usuario. Por lo general, los hosts sin capacidad de respuesta o que tienen error se deben a un problema más serio, por ejemplo, que los hosts o agentes hayan presentado error o que exista un problema de redes.

Otra causa probable de este problema se debe a que su clúster contiene máquinas virtuales que tienen mucha mayor reserva de memoria o de CPU que las otras. La directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) está basada en el cálculo de un tamaño de ranura que consta de dos componentes: las reservas de CPU y memoria de una máquina virtual. Si el cálculo de este tamaño de ranura está sesgado por máquinas virtuales con valores atípicos, la directiva de control de admisión puede volverse demasiado restrictiva y redundar en un clúster rojo. En este caso, puede usar las opciones avanzadas de vSphere HA para reducir el tamaño de ranura, emplear una directiva de control de admisión diferente o modificar la directiva para que tolere menos errores del host.

Solución

Compruebe que todos los hosts en el clúster estén en buen estado, es decir, conectados, no en modo de mantenimiento y sin errores de vSphere HA. El control de admisión de vSphere HA solo considera recursos de hosts en buen estado.

No se puede encender la máquina virtual debido a insuficientes recursos de conmutación por error

Puede que reciba un error de `not enough failover resources` (no hay suficientes recursos de conmutación por error) cuando intenta encender una máquina virtual en un clúster de vSphere HA.

Problema

Si selecciona la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) y surgen ciertos problemas, puede que no sea posible encender una máquina virtual debido a recursos insuficientes.

Causa

Este problema puede tener varias causas.

- Los hosts en el clúster están desconectados, en modo de mantenimiento, no respondiendo o tienen un error de vSphere HA.

  Comúnmente los hosts en modo desconectado y de mantenimiento se deben a una acción provocada por el usuario. Por lo general, los hosts sin capacidad de respuesta o que tienen error se producen por un problema más serio, por ejemplo, que los hosts o agentes hayan generado errores o que exista un problema de redes).

- El clúster contiene máquinas virtuales que poseen reservas de memoria o CPU mucho mayores que las otras.

  La directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host) está basada en el cálculo de un tamaño de ranura que consta de dos componentes: las reservas de CPU y memoria de una máquina virtual. Si el cálculo de este tamaño de ranura está sesgado por máquinas virtuales con valores atípicos, la directiva de control de admisión puede volverse demasiado restrictiva y provocar que no se puedan encender las máquinas virtuales.

- No hay ranuras libres en el clúster.

  Se producen problemas si no hay ranuras libres en el clúster o si el encendido de una máquina virtual hace que el tamaño de ranura aumente, ya que tiene una reserva mayor que las máquinas virtuales existentes. En cualquier caso, debe usar las opciones avanzadas de vSphere HA para reducir el tamaño de ranura, emplear una directiva de control de admisión diferente o modificar la directiva para que tolere menos errores del host.

Solución

Vea el panel **Advanced Runtime Info** (Información de tiempo de ejecución avanzada) que aparece en la sección de vSphere HA de la pestaña **Monitor** (Supervisar) del clúster en vSphere Web Client. El panel de información muestra el tamaño de ranura y cuántas ranuras disponibles hay en el clúster. Si el tamaño de ranura parece ser demasiado grande, haga clic en la pestaña **Resource Allocation** (Asignación de recursos) del clúster y ordene las máquinas virtuales por reserva a fin de determinar cuál tiene las mayores reservas de CPU y memoria. Si hay máquinas virtuales con valores atípicos y muchas mayores reservas que otras, considere usar una directiva de control de admisión de vSphere HA diferente (como Percentage of Cluster Resources Reserved [Porcentaje de recursos del clúster reservados]) o utilice las opciones avanzadas de vSphere HA para colocar un tope absoluto en el tamaño de ranura. Sin embargo, ambas opciones aumentan el riesgo de fragmentación de recursos.

Aparecen menos ranuras disponibles de lo esperado

El cuadro Advanced Runtime Info (Información de tiempo de ejecución avanzada) podría mostrar una menor cantidad de ranuras disponibles en el clúster de lo que espera.

Problema

Cuando seleccione la directiva de control de admisión Host Failures Cluster Tolerates (Tolerancias del clúster para errores del host), vea el panel de **Advanced Runtime Info** (Información de tiempo de ejecución avanzada) que aparece en la sección de vSphere HA de la pestaña **Monitor** (Supervisar) del clúster en vSphere Web Client. Este panel muestra información sobre el clúster, incluida la cantidad de ranuras disponibles para encender máquinas virtuales adicionales en el clúster. Esta cantidad puede ser menor de lo esperado en ciertas condiciones.

Causa

El tamaño de ranura se calcula utilizando las reservas de mayor tamaño más la sobrecarga de memoria de cualquier máquina virtual encendida en el clúster. Sin embargo, el control de admisión de vSphere HA considera solo los recursos en un host que están disponibles para máquinas virtuales. Esta cantidad es menor que la cantidad total de recursos físicos en el host, debido a que hay algo de sobrecarga.

Solución

Si es posible, reduzca las reservas de máquina virtual y use las opciones avanzadas de vSphere HA para disminuir el tamaño de ranura o bien utilice una directiva de control de admisión diferente.

Solucionar problemas de almacenes de datos de latidos

Cuando el host principal en un clúster de vSphere HA ya no puede comunicarse con un host subordinado a través de la red de administración, el host principal utiliza la verificación de latido del almacén de datos para determinar si el host subordinado puede haber tenido un error o si está en una partición de red. Si el host subordinado dejó de verificar el latido del almacén de datos, se considera que ese host tiene un error y sus máquinas virtuales se reinician en otro lado.

vCenter Server selecciona automáticamente un conjunto preferido de almacenes de datos para la verificación de latido. Esta selección se hace con el objetivo de maximizar la cantidad de hosts que tienen acceso a un almacén de datos determinado y minimizar la probabilidad de que la copia de seguridad de los almacenes de datos seleccionados la realice la misma matriz o el servidor NFS. En la mayoría de los casos, esta selección no debe cambiar. Para ver cuáles almacenes de datos ha seleccionado vSphere HA para usar, en vSphere Web Client puede ir a la pestaña **Supervisar** del clúster y seleccionar vSphere HA y Latido. Aquí solo hay disponibles almacenes de datos montados por al menos dos hosts.

Nota Si el único almacenamiento compartido accesible para todos los hosts del clúster es vSAN, no existe un almacén de datos de latidos disponible.

No se selecciona el almacén de datos preferido del usuario

Es posible que vCenter Server no seleccione un almacén de datos que especifique como preferencia para la verificación de latidos del almacenamiento de vSphere HA.

Problema

Puede especificar los almacenes de datos preferidos para la verificación de latidos del almacenamiento y, según esta preferencia, vCenter Server determina el conjunto final de almacenes de datos que se va a usar. Sin embargo, puede que vCenter Server no seleccione los almacenes de datos que especifique.

Causa

Este problema puede producirse en los siguientes casos:

- La cantidad especificada de almacenes de datos es más que la necesaria. vCenter Server selecciona el número óptimo de almacenes de datos que se requieren en la preferencia establecida por el usuario y pasa por alto el resto.
- Un almacén de datos especificado no es óptimo para la accesibilidad del host y la redundancia de respaldo del almacenamiento. Más específicamente, puede que el almacén de datos no se seleccione si está accesible solo para un pequeño conjunto de hosts en el clúster. También podría seleccionarse un almacén de datos si está en el mismo LUN o el mismo servidor NFS que los almacenes de datos que vCenter Server ya ha seleccionado.
- No se puede acceder a un almacén de datos debido a errores de almacenamiento, por ejemplo, todas las rutas de acceso inactivas (All Paths Down, APD) o pérdida permanente de dispositivos (Permanent Device Loss, PDL) de la matriz de almacenamiento.
- Si el clúster contiene una partición de red o si un host está inaccesible o aislado, el host sigue usando los almacenes de datos de latidos existentes incluso si las preferencias de usuario cambian.

Solución

Compruebe que todos los hosts en el clúster estén accesibles y que tengan el agente de vSphere HA funcionando. También, asegúrese de que los almacenes de datos especificados estén accesibles para la mayoría, sino todos, los hosts del clúster y que los almacenes de datos estén en LUN o servidores NFS diferentes.

Errores en el desmontaje o la eliminación de un almacén de datos

Cuando se intenta desmontar o eliminar un almacén de datos, se produce un error en la operación.

Problema

Se produce un error en la operación para desmontar o eliminar un almacén de datos si el almacén de datos tiene archivos abiertos. Para estas operaciones de usuarios, el agente de vSphere HA cierra todos los archivos que tiene abiertos, por ejemplo archivos de latido. Si vCenter Server no puede acceder al agente o el agente no puede purgar E/S pendientes para cerrar los archivos, se acciona el error `El agente de HA en el host '{hostName}' presentó error al poner en modo inactivo la actividad del archivo en el almacén de datos {dsName}.`

Causa

Si el almacén de datos que se va a desmontar o eliminar se utiliza para verificación de latidos, vCenter Server lo excluye de la verificación de latidos y selecciona uno nuevo. Sin embargo, el agente no recibe los almacenes de datos con latido actualizado si no se puede acceder a él, es decir, si el host está aislado o en una partición de red. En dichos casos, los archivos de latido no se cierran y se produce un error de operación de usuario. La operación también puede presentar error si no se puede acceder al almacén de datos debido a errores de almacenamiento, como caída de todas las rutas de acceso.

Nota Cuando elimina un almacén de datos de VMFS, este almacén se quita de todos los hosts en el inventario. Por lo tanto, si hay hosts en un clúster de vSphere HA a los que no se puede acceder o que no tienen acceso al almacén de datos, hay error en la operación.

Solución

Asegúrese de que el almacén de datos esté accesible y que se pueda acceder a los hosts afectados.

Solucionar problemas de respuesta a errores de vSphere HA

vSphere HA ofrece alta disponibilidad para máquinas virtuales agrupando en un clúster las máquinas virtuales y los hosts en los que residen. Se supervisan los hosts en el clúster y, en caso de un error, las máquinas virtuales en un host con errores se reinician en hosts alternativos.

Existen varios motivos por los cuales es posible que máquinas virtuales afectadas no se reinicien y, si esto ocurre, deberá solucionar los problemas para determinar la causa.

Incorrect Virtual Machine Protection State

A virtual machine in a vSphere HA cluster is reported as vSphere HA unprotected although it has been powered on for several minutes.

Problema

When a virtual machine is powered on for several minutes, yet its vSphere HA protection state remains as unprotected, if a failure occurs, vSphere HA might not attempt to restart the virtual machine.

Causa

vCenter Server reports a virtual machine as protected after the vSphere HA primary host that is responsible for the virtual machine has saved to disk the information that the virtual machine must be restarted after a failure. This process can fail for a number of reasons.

- vSphere HA primary host has not been elected or vCenter Server is unable to communicate with it.

In this situation, vCenter Server reports the vSphere HA host state for the cluster hosts as Agent Unreachable or Agent Uninitialized and reports a cluster configuration problem that a primary host has not been found.

- Multiple primary hosts exist and the one with which vCenter Server is communicating is not responsible for the virtual machine.

  Problems occur when vCenter Server is in contact with a primary host, but due to a management network partition, there are multiple primary hosts, and the agent with which vCenter Server is communicating is not responsible for the virtual machine. This situation is likely if vCenter Server is reporting the vSphere HA state of some hosts as network partitioned.

- Agent is unable to access the datastore on which the configuration file of the virtual machine is stored.

  vCenter Server might be in contact with the vSphere HA primary host that owns the virtual machine, but the agent is unable to access the datastore on which the configuration file of the virtual machine is stored. This situation can occur if an all paths down condition affects all hosts in the cluster.

Solución

1 Determine whether vCenter Server is in contact with a vSphere HA primary host, and if not, address this problem.

2 If vCenter Server is in contact with a primary host, determine whether there is a network partition, and if so, address that problem.

3 If the problem persists, determine if other virtual machines that use the same datastore for their configuration files are also unprotected.

4 If these virtual machines are unprotected, verify that the vSphere HA primary host can access the datastore.

5 If none of the previous steps resolves the problem, restore protection by reconfiguring vSphere HA on the host on which the virtual machine is running.

Error de reinicio de la máquina virtual

Después de un error en un host o máquina virtual, puede que no sea posible reiniciar una máquina virtual.

Problema

Cuando hay error en un host o una máquina genera errores mientras su host continúa en ejecución, puede que la máquina virtual no se reinicie o lo haga solo después de un prolongado retraso.

Causa

Puede que vSphere HA no reinicie una máquina virtual después de un error o que retrase su reinicio por varios motivos.

- La máquina virtual no tiene protección de vSphere HA en el momento que se produjo el error.
- Insuficiente capacidad disponible en hosts con los cuales la máquina virtual es compatible.
- vSphere HA intentó reiniciar la máquina virtual, pero encontró un error fatal cada vez que lo intentó.
- El almacenamiento compartido de su clúster es vSAN y uno de los archivos de la máquina virtual quedó inaccesible debido a la existencia de más de la cantidad especificada de errores del host.
- Reinicio realizado correctamente.

Solución

Para evitar errores en el reinicio de máquinas virtuales, compruebe que las máquinas virtuales queden protegidas con vSphere HA después de que se encienden. Igualmente, asegúrese de que su configuración de control de admisión coincida con sus expectativas de reinicio en caso de que se produzca un error. La maximización de la compatibilidad entre máquinas virtuales y hosts en el clúster también puede reducir la probabilidad de errores en el reinicio.

Nota Para obtener información sobre los factores que vSphere HA considera para los reinicios de máquinas virtuales, consulte "Determinación de respuestas a problemas del host" en *Disponibilidad de vSphere*.

Troubleshooting vSphere Fault Tolerance in Network Partitions

When a vSphere HA cluster experiences a failure of the network that vSphere uses for inter-agent communication (the management network), a subset of the cluster's hosts might be unable to communicate with other cluster hosts. In this case, the set of hosts that can communicate with each other are considered to be in a network partition.

A cluster partition impedes cluster management functions such as vMotion and can impact vSphere HA’s ability to monitor and restart virtual machines after a failure. This condition must be corrected as soon as possible.

Network partitions also degrade the functionality of vSphere Fault Tolerance. For example, in a partitioned cluster, a Primary VM (or its Secondary VM) could end up in a partition managed by a primary host that is not responsible for the virtual machine. When a Secondary VM must be restarted, vSphere HA does so only if the Primary VM is in a partition managed by the primary host responsible for it. Ultimately, you must correct the network partition, but until that is possible, you must troubleshoot and correct any problems that arise with your fault-tolerant virtual machines to ensure that they are properly protected.

Primary VM Remains in the Need Secondary State

A fault tolerant Primary VM can remain in the `need secondary` state even though sufficient resources are available to start the Secondary VM.

Problema

vSphere HA might not restart the Secondary VM of a vSphere Fault Tolerance (FT) virtual machine pair even though there are sufficient resources available.

Causa

To restart a Secondary VM, vSphere HA requires that the Primary VM be running on a host that is in the same partition as the one containing the vSphere HA primary host responsible for the FT pair. In addition, the vSphere HA agent on the Primary VM's host must be operating correctly. If these conditions are met, FT also requires that there be at least one other host in the same partition that is compatible with the FT pair and that has a functioning vSphere HA agent.

Solución

To fix this condition, check the vSphere HA host states reported by vCenter Server. If hosts are identified as partitioned, isolated, or unreachable, resolve the problem before proceeding. In some situations, you can resolve a restart problem by reconfiguring vSphere HA on the host that vCenter Server is reporting as the primary host. However, in most situations, this step is insufficient, and you must resolve all host state problems.

After you have addressed any host state problems, check if there are any hosts in the cluster other than the Primary VM's that are compatible with the FT virtual machine pair. You can determine compatibility by trying to migrate the Primary VM to other hosts. Address any incompatibilities that are discovered.

Problemas de comportamiento de cambio de roles

vCenter Server puede informar que la máquina virtual principal de un par de máquinas virtuales de vSphere Fault Tolerance está apagada, pero la máquina virtual secundaria está encendida.

Problema

Después de que se produce una conmutación por error, vCenter Server podría informar de forma incorrecta que la máquina virtual principal está apagada y registrada en su host original y que la máquina virtual secundaria está encendida y registrada en su host original.

Causa

Este error se produce cuando vCenter Server no puede comunicarse con los hosts en los cuales la máquina virtual principal y la máquina virtual secundaria se ejecutan realmente. vCenter Server informa que estos hosts no están respondiendo y que el problema persiste hasta que vCenter Server puede comunicarse con los hosts.

Solución

Para solucionar este problema, resuelva el problema de redes que está impidiendo que vCenter Server se comunique con los hosts en el clúster.

Solucionar problemas de Protección de componentes de la máquina virtual

Si habilita la función Protección de componentes de la máquina virtual (VM Component Protection, VMCP) para el clúster de vSphere HA, esta ofrece protección contra errores de accesibilidad del almacén de datos que pueden afectar a una máquina virtual que se ejecuta en uno de los hosts del clúster.

Si no se ejecuta la respuesta que debe hacer VMCP ante dicho error según lo configurado, se debe solucionar el problema para determinar la causa.

Datastore Inaccessibility Is Not Resolved for a VM

When a datastore becomes inaccessible, VMCP might not terminate and restart the affected virtual machines.

Problema

When an All Paths Down (APD) or Permanent Device Loss (PDL) failure occurs and a datastore becomes inaccessible, VMCP might not resolve the issue for the affected virtual machines.

Causa

In an APD or PDL failure situation, VMCP might not terminate a virtual machine for the following reasons:

- VM is not protected by vSphere HA at the time of failure.
- VMCP is disabled for this virtual machine.

Furthermore, if the failure is an APD, VMCP might not terminate a VM for several reasons:

- APD failure is corrected before the VM was terminated.
- Insufficient capacity on hosts with which the virtual machine is compatible
- During a network partition or isolation, the host affected by the APD failure is not able to query the primary host for available capacity. In such a case, vSphere HA defers to the user policy and terminates the VM if the VM Component Protection setting is aggressive.
- vSphere HA terminates APD-affected VMs only after the following timeouts expire:
  - APD timeout (default 140 seconds).
  - APD failover delay (default 180 seconds). For faster recovery, this can be set to 0.

    Nota Based on these default values, vSphere HA terminates the affected virtual machine after 320 seconds (APD timeout + APD failover delay)

Solución

To address this issue, check and adjust any of the following:

- Insufficient capacity to restart the virtual machine
- User-configured timeouts and delays
- User settings affecting VM termination
- VM Component Protection policy
- Host monitoring or VM restart priority must be enabled

Solucionar problemas de recursos

6

Los temas de solución de problemas de administración de recursos proporcionan soluciones para posibles problemas con los que podría encontrarse al usar los hosts y almacenes de datos en un clúster de vSphere DRS o vSphere Storage DRS.

Este capítulo incluye los siguientes temas:

Solucionar problemas de Storage DRS

Los temas de solución de problemas de Storage DRS ofrecen soluciones a posibles problemas que se podrían encontrar al usar almacenes de datos con Storage DRS habilitado en un clúster de almacenes de datos.

Storage DRS está deshabilitado en un disco virtual

Incluso cuando Storage DRS esté habilitado para un clúster de almacenes de datos, puede que esté deshabilitado en algunos discos virtuales en el clúster de almacenes de datos.

Problema

Ha habilitado Storage DRS para un clúster de almacenes de datos, pero Storage DRS está deshabilitado en uno o más discos de máquina virtual en el clúster de almacenes de datos.

Causa

Los siguientes escenarios pueden hacer que Storage DRS se deshabilite en un disco virtual.

- El archivo de intercambio de una máquina virtual es local para el host (el archivo de intercambio está almacenado en un almacén de datos local que se encuentra en el host).
  El archivo de intercambio no puede reubicarse y Storage DRS se deshabilita para el disco del archivo de intercambio.
- Se especifica cierta ubicación para el archivo de intercambio `.vmx` de una máquina virtual.
  El archivo de intercambio no puede reubicarse y Storage DRS se deshabilita en el disco del archivo de intercambio `.vmx`.

- La operación de reubicación o de Storage vMotion se encuentra deshabilitada actualmente para la máquina virtual en vCenter Server (por ejemplo, debido a que hay otras operaciones de vCenter Server en curso en la máquina virtual). Storage DRS está deshabilitado hasta que se vuelve a habilitar la operación de reubicación o de Storage vMotion en vCenter Server.
- El disco de inicio de una máquina virtual se protege mediante vSphere HA y si se reubica, habrá una pérdida de protección de vSphere HA.
- El disco es un archivo CD-ROM/ISO.
- Si el disco es independiente, Storage DRS se deshabilita, excepto en caso de reubicación o colocación de clones.
- Si la máquina virtual tiene archivos de sistema en un almacén de datos separado del almacén de datos de inicio (heredado), Storage DRS se deshabilita en el disco de inicio. Si utiliza Storage vMotion para migrar de forma manual el disco de inicio, todos los archivos de sistema en diferentes almacenes de datos estarán ubicados en el almacén de datos de destino y Storage DRS estará habilitado en el disco de inicio.
- Si la máquina virtual tiene un disco cuyos archivos de base de base/rehacer están distribuidos entre almacenes de datos separados (heredados), se deshabilita Storage DRS para el disco. Si utiliza Storage vMotion para migrar de forma manual el disco, todos los archivos en diferentes almacenes de datos estarán ubicados en el almacén de datos de destino y Storage DRS estará habilitado en el disco de inicio.
- La máquina virtual tiene discos ocultos (como discos en instantáneas anteriores, no en la instantánea actual). Debido a esta situación, Storage DRS se deshabilitará en la máquina virtual.
- La máquina virtual es una plantilla.
- La máquina virtual tiene habilitado vSphere Fault Tolerance.
- La máquina virtual está compartiendo archivos entre sus discos.
- La máquina virtual está sometida a colocación mediante Storage DRS con almacenes de datos especificados manualmente.

Solución

Resuelva el problema que está haciendo que Storage DRS se deshabilite en el disco.

El almacén de datos no puede entrar en modo de mantenimiento

Coloca un almacén de datos en modo de mantenimiento cuando debe sacarlo de uso para brindarle servicio. Un almacén de datos entra o sale del modo de mantenimiento solo como resultado de una solicitud de usuario.

Problema

Un almacén de datos en un clúster de almacenes de datos no puede entrar en modo de mantenimiento. El estado Entering Maintenance Mode (Entrando en modo de mantenimiento) permanece en el 1 %.

Causa

Uno o más discos en el almacén de datos no puede migrarse con Storage vMotion. Esta condición puede producirse en las siguientes instancias.

- Storage DRS está deshabilitado en el disco.
- Las reglas de Storage DRS impiden que Storage DRS haga recomendaciones de migración para el disco.

Solución

- Si Storage DRS está deshabilitado, habilítelo o determine por qué está deshabilitado. Consulte Storage DRS está deshabilitado en un disco virtual para conocer los motivos por los cuales Storage DRS podría estar deshabilitado.
- Si las reglas de Storage DRS están impidiendo que Storage DRS haga recomendaciones de migración, puede eliminar o deshabilitar reglas particulares.
  a Desplácese hasta el clúster de almacenes de datos en el navegador de objetos de vSphere Web Client.
  b Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
  c En Configuration (Configuración), seleccione **Rules** (Reglas) y haga clic en la regla.
  d Haga clic en **Remove** (Quitar).
- De manera alternativa, si las reglas de Storage DRS están impidiendo que haga recomendaciones de migración, puede configurar la opción avanzada de Storage DRS IgnoreAffinityRulesForMaintenance en 1.
  a Desplácese hasta el clúster de almacenes de datos en el navegador de objetos de vSphere Web Client.
  b Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
  c Seleccione **SDRS** y haga clic en **Edit** (Editar).
  d En **Advanced Options (Opciones avanzadas) > Configuration Parameters (Parámetros de configuración)**, haga clic en **Add** (Agregar).
  e En la columna Option (Opción), introduzca **`IgnoreAffinityRulesForMaintenance`**.
  f En la columna Value (Valor), introduzca **1** para habilitar la opción.
  g Haga clic en **OK** (Aceptar).

Storage DRS no puede funcionar en un almacén de datos

Storage DRS genera una alarma para indicar que no puede operar en el almacén de datos.

Problema

Storage DRS genera un evento y una alarma y Storage DRS no puede operar.

Causa

Los siguientes escenarios pueden hacer que vCenter Server deshabilite Storage DRS para un almacén de datos.

- El almacén de datos se comparte entre varios centros de datos.

  Storage DRS no se admite en almacenes de datos que se comparten entre varios centros de datos. Esta configuración puede producirse cuando un host en un centro de datos monta un almacén de datos en otro centro de datos, o cuando un host que usa el almacén de datos se mueve a un centro de datos diferente. Cuando un almacén de datos se comparte entre varios centros de datos, el equilibrio de carga de E/S de Storage DRS se deshabilita para el clúster de almacenes de datos completo. Sin embargo, el equilibrio de espacio de Storage DRS permanece activo para todos los almacenes de datos en el clúster de almacenes de datos que no estén compartidos entre centros de datos.

- El almacén de datos está conectado a un host no compatible.

  Storage DRS no es compatible en ESX/ESXi 4.1 ni hosts con versiones anteriores.

- El almacén de datos está conectado a un host que no ejecuta E/S de Storage I/O Control.

Solución

- El almacén de datos debe estar visible solo en un centro de datos. Mueva los hosts al mismo centro de datos o desmonte el almacén de datos de los hosts que se encuentran en otros centros de datos.
- Asegúrese de que todos los hosts asociados con el clúster de almacenes de datos tengan ESXi 5.0 o una versión posterior.
- Asegúrese de que todos los hosts asociados con el clúster de almacenes de datos tengan habilitado Storage I/O Control.

Se producen errores al mover varias máquinas virtuales a un clúster de almacenes de datos

La migración de más de un almacén de datos a un clúster de almacenes de datos produce un mensaje de error después de que la primera máquina virtual se ha movido correctamente al clúster de almacenes de datos.

Problema

Cuando intenta migrar varias máquinas virtuales a un clúster de almacenes de datos, algunas máquinas migran correctamente, pero hay error en la migración de máquinas posteriores. vCenter Server muestra el mensaje de error, `Insufficient Disk Space on Datastore` (No hay suficiente espacio en disco en el almacén de datos).

Causa

Hasta que se aplique cada recomendación de colocación, los recursos de espacio parecen estar disponibles para Storage DRS. Por lo tanto, puede que Storage DRS vuelva a asignar recursos de espacio a solicitudes posteriores de espacio.

Solución

Reintente las operaciones de migración con error de a una a la vez y asegúrese de aplicar cada recomendación antes de solicitar la próxima migración.

Storage DRS genera error durante la creación de una máquina virtual

Cuando se crea o clona una máquina virtual en un clúster de almacenes de datos, Storage DRS podría generar un error.

Problema

Cuando se intenta crear o clonar una máquina virtual en un clúster de almacenes de datos, puede que se reciba el mensaje de error, `Operation Not Allowed in the Current State` (Operación no permitida en el estado actual).

Causa

Cuando se crea una máquina virtual en un almacén de datos con Storage DRS habilitado, Storage DRS comprueba si hay infracciones de reglas. Si Storage DRS no puede crear los discos de la nueva máquina virtual cumpliendo con las reglas, genera un error. El error se produce debido a que Storage DRS no puede hacer referencia a la máquina virtual, la que se encuentra en proceso de creación y aún no existe.

Solución

Modifique o elimine la reglas y vuelva a intentar la operación de creación o clonación de la máquina virtual.

Storage DRS está habilitado en una máquina virtual implementada desde una plantilla de OVF

Storage DRS está habilitado en una máquina virtual que se implementó desde una plantilla de OVF que tiene Storage DRS deshabilitado. Esto puede ocurrir cuando se implementa una plantilla de OVF en un clúster de almacenes de datos.

Problema

Cuando se implementa una plantilla de OVF con Storage DRS deshabilitado en un clúster de almacenes de datos, la máquina virtual resultante tiene habilitado Storage DRS.

Causa

vSphere Web Client aplica el nivel de automatización predeterminado del clúster de almacenes de datos a máquinas virtuales implementadas a partir de una plantilla de OVF.

Solución

1 Para cambiar de forma manual el nivel de automatización de la máquina virtual, desplácese al clúster de almacenes de datos en el navegador de objetos de vSphere Web Client.
2 Haga clic en la pestaña **Manage** (Administrar) y seleccione **Settings** (Configuración).
3 Seleccione **VM Overrides** (Reemplazos por máquina virtual) y haga clic en **Add** (Agregar).
4 Seleccione la máquina virtual y haga clic en **OK** (Aceptar).
5 En el menú desplegable **Keep VMDKs Together** (Mantener VMDK juntas), seleccione **No** y haga clic en **OK** (Aceptar).

Aparece varias veces un error de infracción de regla de Storage DRS

Cuando intenta colocar un almacén de datos en modo de mantenimiento, podría parecer que el mismo error de infracción de regla de afinidad o antiafinidad se indica más de una vez en el cuadro de diálogo Faults (Errores).

Problema

Parece que el cuadro de diálogo Faults (Errores) muestra varias instancias de errores idénticos, pero en realidad, cada error se refiere a un almacén de datos diferente. El cuadro de diálogo Faults (Errores) no enumera los nombres del almacén de datos, lo que hace que los errores parezcan ser redundantes.

Solución

El cuadro de diálogo Faults (Errores) muestra un error de infracción de regla separado para cada almacén de datos que se considera para su colocación. Si desea que el almacén de datos entre en modo de mantenimiento, elimine la regla que evita la migración de la máquina virtual.

Reglas de Storage DRS que no se eliminan del clúster de almacenes de datos

Las reglas de afinidad o antiafinidad que se aplican a una máquina virtual no se eliminan cuando quita la máquina virtual de un clúster de almacenes de datos.

Problema

Cuando elimina una máquina virtual de un clúster de almacenes de datos, y esa máquina virtual está sujeta a una regla de afinidad o antiafinidad en un clúster de almacenes de datos, la regla permanece. Esto le permite almacenar configuraciones de máquina virtual en diferentes clústeres de almacenes de datos. Si la máquina virtual se vuelve a mover al clúster de almacenes de datos, se aplica la regla. No puede eliminar la regla después de que quita la máquina virtual del clúster de almacenes de datos.

Causa

vCenter Server conserva reglas para una máquina virtual que se quita de un clúster de almacenes de datos en caso de que la máquina virtual permanezca en el inventario de vCenter Server.

Solución

Para eliminar una regla de la configuración de un clúster de almacenes de datos, debe eliminar la regla antes de quitar del clúster de almacenes de datos la máquina virtual a la cual se aplica la regla.

1. En vSphere Web Client, desplácese al clúster de almacenes de datos.
2. Haga clic en la pestaña **Manage** (Administrar) y seleccione **Settings** (Configuración).
3. En Configuration (Configuración), haga clic en **Rules** (Reglas).
4. Seleccione la regla que va a eliminar y haga clic en **Remove** (Quitar).
5. Haga clic en **OK** (Aceptar).

No se generan recomendaciones alternativas de colocación de Storage DRS

Cuando crea, clona o reubica una máquina virtual, Storage DRS genera solo una recomendación de colocación.

Problema

Storage DRS genera una sola recomendación de colocación cuando crea, clona o reubica una máquina virtual. No se proporcionan recomendaciones alternativas cuando se esperan varias de ellas.

Causa

Si el host de destino especifica de forma explícita la ubicación del archivo de intercambio de la máquina virtual como un almacén de datos en el clúster de almacenes de datos de destino, los discos que se colocarán en ese clúster no forman un grupo único de afinidades. Storage DRS genera recomendaciones de colocación alternativas solo para un único elemento o un grupo único de afinidades.

Solución

Acepte la recomendación única. Para obtener varias, seleccione un host de destino que no especifique que la ubicación del archivo de intercambio de la máquina virtual esté en un almacén de datos que se encuentre en el clúster de almacenes de datos de destino.

Error al aplicar recomendaciones de Storage DRS

Storage DRS genera espacio para recomendaciones de equilibrio de carga de E/S, pero se produce un error al aplicar las recomendaciones.

Problema

Cuando se aplican recomendaciones de Storage DRS para el espacio o el equilibrio de carga de E/S, se producen errores en la operación.

Causa

Los siguientes escenarios pueden impedirle que aplique las recomendaciones de Storage DRS.

- Es posible que se haya accionado una alarma de Thin Provisioning Threshold Crossed (Se cruzó el umbral de aprovisionamiento fino) del almacén de datos de destino, que indica que el almacén de datos se está quedando sin espacio y que no se migrarán máquinas virtuales al almacén de datos.
- Es posible que el almacén de datos de destino esté en modo de mantenimiento o que esté entrando en este modo.

Solución

- Solucione el problema que accionó la alarma Thin Provisioning Threshold Crossed (Se cruzó el umbral de aprovisionamiento fino).
- Compruebe que el almacén de datos de destino no esté en modo de mantenimiento ni que esté entrando en este modo.

Solucionar problemas de Storage I/O Control

Los temas de solución de problemas de Storage I/O Control ofrecen soluciones para posibles problemas que podrían encontrarse al usar Storage I/O Control con almacenes de datos.

Host no compatible conectado a un almacén de datos

En vSphere Web Client, se activa una alarma cuando vCenter Server detecta que una carga de trabajo de un host podría estar afectando el rendimiento.

Problema

Se activa la alarma **Pre-4.1 host connected to SIOC-enabled datastore** (Host previo a 4.1 conectado a un almacén de datos con SIOC habilitado).

Causa

El almacén de datos tiene habilitado Storage I/O Control, pero Storage I/O Control no puede controlarlo completamente debido a la carga de trabajo externa.

Esta condición puede producirse si el almacén de datos con Storage I/O Control habilitado está conectado a un host que no es compatible con Storage I/O Control.

Solución

Asegúrese de que todos los hosts que estén conectado al almacén de datos sean compatibles con Storage I/O Control.

Se detectó una carga de trabajo sin administrar en el almacén de datos

En vSphere Web Client, se activa una alarma cuando vCenter Server detecta que una carga de trabajo de un host podría estar afectando el rendimiento.

Problema

Se activó la alarma **Unmanaged workload is detected on the datastore** (Se detectó carga de trabajo sin administrar en el almacén de datos).

Causa

La matriz se comparte con cargas de trabajo que no son de vSphere o está realizando tareas del sistema, como replicación.

Solución

No hay solución. vCenter Server no reduce la cantidad total de E/S que se envía hacia la matriz, pero sigue aplicando recursos compartidos.

No es posible ver gráficos de rendimiento para un almacén de datos

Los gráficos de rendimiento para un almacén de datos no aparecen en la pestaña Performance (Rendimiento).

Problema

No puede ver gráficos de rendimiento para un almacén de datos en la pestaña **Performance** (Rendimiento) en vSphere Web Client.

Causa

Storage I/O Control está deshabilitado para el almacén de datos.

Solución

1 Desplácese hasta el almacén de datos en el navegador de objetos de vSphere Web Client.

2 Haga clic con el botón derecho en el almacén de datos y seleccione **Configure Storage I/O Control** (Configurar Storage I/O Control).

3 Seleccione la casilla de verificación **Enable Storage I/O Control** (Habilitar Storage I/O Control).

4 Haga clic en **OK** (Aceptar).

No se puede habilitar Storage I/O Control en un almacén de datos

Storage I/O Control está deshabilitado en un almacén de datos y no puede habilitarse.

Problema

No puede habilitar Storage I/O Control en un almacén de datos.

Causa

Los siguientes motivos podrían impedir que habilite Storage I/O Control en un almacén de datos.

- Al menos un host que está conectado al almacén de datos no ejecuta ESX/ESXi 4.1 o una versión posterior.
- No tiene la licencia apropiada para habilitar Storage I/O Control.

Solución

- Verifique que los hosts conectados al almacén de datos tengan ESX/ESXi 4.1 o una versión posterior.
- Compruebe que tiene la licencia apropiada para habilitar Storage I/O Control.

Solucionar problemas de almacenamiento

7

Los temas de solución de problemas de almacenamiento ofrecen soluciones a posibles problemas que se podrían encontrar al usar vSphere en diferentes entornos de almacenamiento, incluidos SAN, vSAN o Virtual Volumes.

Este capítulo incluye los siguientes temas:

Solucionar problemas de visualización del almacenamiento de SAN

Cuando se utiliza vSphere Web Client para ver dispositivos de almacenamiento SAN o iSCSI de canal de fibra, es posible que no se puedan ver todos los dispositivos disponibles en el host. Existen varias tarea de solución de problemas que pueden realizarse para resolver problemas de visualización de almacenamiento.

Solucionar problemas de visualización del almacenamiento de canal de fibra

Si los dispositivos de almacenamiento de canal de fibra no se muestran correctamente en vSphere Web Client, realice tareas de solución de problemas.

Tabla 7-1. Solucionar problemas de la visualización de LUN de canal de fibra

Tarea de solución de problemas	Descripción
Comprobar la conectividad de los cables.	Si no ve un puerto, el problema podría ser conectividad de cables. Revise primero los cables. Asegúrese de que los cables estén conectados a los puertos y una luz de vínculo indica que la conexión es buena. Si cada extremo del cable no muestra una luz que indica un buen vínculo, sustituya el cable.
Comprobar zonificación.	La zonificación limita el acceso a dispositivos de almacenamiento específicos, aumenta la seguridad y disminuye el tráfico a través de la red. Algunos proveedores de almacenamiento también permiten solo zonas con iniciador único. En ese caso, un HBA puede estar en varias zonas para un solo destino. Otros proveedores permiten zonas con varios iniciadores. Consulte la documentación de su proveedor de almacenamiento para requisitos de zonificación. Use el software del conmutador SAN para configurar y administrar la zonificación.
Comprobar la configuración de control de acceso.	■ El complemento MASK_PATH le permite evitar que su host tenga acceso a una matriz de almacenamiento específica o LUN específicos en una matriz de almacenamiento. Si su host detecta dispositivos y rutas de acceso a los que no desea que acceda el host, es posible que la máscara de la ruta de acceso se haga configurado incorrectamente. ■ Para un arranque desde una SAN, asegúrese de que cada host vea solo los LUN necesarios. No permita que ningún host vea un LUN de arranque distinto al propio. Use un software del sistema de almacenamiento para cerciorarse de que el host pueda ver solo los LUN debidos. ■ Asegúrese de que el parámetro **Disk.MaxLUN** le permita visualizar el LUN que espera ver. Para obtener información sobre el parámetro, consulte la documentación de *Almacenamiento de vSphere*.
Comprobar instalación del procesador de almacenamiento.	Si una matriz de discos tiene más de un procesador (SP), asegúrese de que el conmutador SAN tenga una conexión a SP que posea los LUN a los que desea tener acceso. En algunas matrices de disco, solo un SP es activo y el otro es pasivo hasta que hay un error. Si está conectado al SP incorrecto (aquel con la ruta de acceso al pasivo), puede que vea los LUN, pero que reciba errores cuando intenta acceder a ellos.
Volver a examinar su HBA.	Realice un nuevo examen cada vez que realice las siguientes tareas: ■ Al crear LUN nuevos en una SAN. ■ Cambie la configuración de la máscara de ruta de acceso en el host. ■ Reconectar un cable. ■ Hacer un cambio a un host en un clúster. Para obtener información, consulte el documento *Almacenamiento de vSphere*.

Solucionar problemas de visualización del almacenamiento de iSCSI

Realice tareas de solución de problemas si los dispositivos de almacenamiento iSCSI no aparecen correctamente en vSphere Web Client.

Tabla 7-2. Solucionar problemas para visualización de LUN iSCSI

Tarea de solución de problemas	Descripción
Comprobar la conectividad de los cables.	Si no ve un puerto, el problema podría ser la conectividad de cables o el enrutamiento. Revise primero los cables. Asegúrese de que los cables estén conectados a los puertos y una luz de vínculo indica que la conexión es buena. Si cada extremo del cable no muestra una luz que indica un buen vínculo, sustituya el cable.
Comprobar la configuración de enrutamiento.	Controle la conectividad entre diferentes subredes en la configuración Ethernet. Si su sistema de ESXi y almacenamiento iSCSI no están en la misma subred, asegúrese de que exista un enrutamiento adecuado entre las subredes. Igualmente, asegúrese de que la máscara de subred y la dirección de la puerta de enlace estén configuradas correctamente en el almacenamiento iSCSI y el iniciador de iSCSI en el host ESXi.
Comprobar la configuración de control de acceso.	Si los LUN esperados no aparecen después del nuevo análisis, es posible que el control de acceso no esté configurado correctamente en el lado del sistema de almacenamiento: ■ Si CHAP está configurado, asegúrese de que esté habilitado en el host ESXi y que coincida con la instalación del sistema de almacenamiento. ■ En caso de que se utilice filtrado basado en IP, asegúrese de que se permita la dirección IP del grupo de puertos de HBA iSCSI o de VMkernel. ■ Si está usando filtrado basado en nombre del iniciador, asegúrese de que sea un nombre de iSCSI calificado y que coincida con la instalación del sistema de almacenamiento. ■ Para un arranque desde una SAN, asegúrese de que cada host vea solo los LUN necesarios. No permita que ningún host vea un LUN de arranque distinto al propio. Use un software del sistema de almacenamiento para cerciorarse de que el host pueda ver solo los LUN debidos. ■ Asegúrese de que la configuración **Disk.MaxLUN** le permita ver el LUN que espera ver. Para obtener información, consulte el documento *Almacenamiento de vSphere*.
Comprobar instalación del procesador de almacenamiento.	Si un sistema de almacenamiento tiene más de un procesador de almacenamiento, asegúrese de que el conmutador SAN tenga una conexión SP que posea los LUN a los que desea tener acceso. En algunos sistemas de almacenamiento, solo un SP es activo y el otro es pasivo hasta que se produce un error. Si está conectado al SP incorrecto (aquel con la ruta de acceso al pasivo), puede que no vea los LUN esperados, o bien podría ver los LUN pero recibir errores cuando intenta acceder a ellos.
Para iSCSI de software y dependiente del hardware, comprobar la configuración de red.	Los adaptadores de software iSCSI y que dependen del hardware en ESXi necesitan que el puerto de red de VMkernel tengan acceso al almacenamiento iSCSI. Los adaptadores usan el VMkernel para transferencia de datos entre el sistema de ESXi y el almacenamiento iSCSI.
Volver a examinar su iniciador de iSCSI.	Realice un nuevo examen cada vez que realice las siguientes tareas: ■ Al crear LUN nuevos en una SAN. ■ Cambiar las máscaras de LUN. ■ Reconectar un cable. ■ Hacer un cambio a un host en un clúster. ■ Cambiar configuración CHAP o agregar nuevas direcciones de detección. Para obtener información, consulte el documento *Almacenamiento de vSphere*.

Solucionar problemas de rendimiento de SAN

Varios factores pueden afectar de forma negativa el rendimiento del almacenamiento en el entorno SAN de ESXi. Entre estos factores figuran las excesivas reservas de SCSI, hiperpaginación de rutas de acceso y una inadecuada profundidad de la cola de LUN.

Para supervisar el rendimiento del almacenamiento en tiempo real, use las utilidades de línea de comandos `resxtop` y `esxtop`. Para obtener más información, consulte la documentación de *Supervisión y rendimiento de vSphere*.

El exceso de reservas de SCSI provoca un rendimiento lento del host

Cuando los dispositivos de almacenamiento no admiten la aceleración de hardware, los hosts ESXi utilizan el mecanismo de reservas de SCSI para ejecutar operaciones en las que se requiere un bloqueo de archivos o de metadatos en VMFS. Las reservas de SCSI bloquean el LUN completo. Excesivas reservas de SCSI por parte de un host pueden provocar degradación de rendimiento en otros servidores que acceden al mismo VMFS.

Problema

Excesivas reservas de SCSI provocan degradación de rendimiento y conflictos de reservas de SCSI.

Causa

Varias operaciones requieren VMFS para usar reservas de SCSI.

- Creación, nueva firma o expansión de un almacén de datos de VMFS
- Encendido de una máquina virtual
- Creación o eliminación de un archivo
- Creación de una plantilla
- Implementación de una máquina virtual desde una plantilla
- Creación de una nueva máquina virtual
- Migración de una máquina virtual con VMotion
- Aumento del tamaño de un archivo, como un disco virtual con aprovisionamiento fino

---

Nota Para dispositivos de almacenamiento que admitan la aceleración de hardware, los hosts utilizan el algoritmo de pruebas y conjuntos atómicos (ATS) para bloquear el LUN. Para obtener más información acerca de la aceleración de hardware, consulte la documentación de *Almacenamiento de vSphere*.

Solución

Para eliminar posibles fuentes de conflictos de reservas de SCSI, siga estas directrices:

- Serialice las operaciones de los LUN compartidos, si es posible, limite la cantidad de operaciones en diferentes hosts que requieren reserva de SCSI al mismo tiempo.
- Aumente la cantidad de LUN y limite la cantidad de hosts que acceden al mismo LUN.
- Reduzca la cantidad de instantáneas. Las instantáneas provocan numerosas reservas de SCSI.
- Reduzca la cantidad de máquinas virtuales por LUN. Siga las recomendaciones en *Valores máximos de configuración*.
- Asegúrese de que tiene el firmware más reciente de HBA entre todos los hosts.
- Asegúrese de que el host tiene el BIOS más reciente.
- Asegure una configuración correcta de Modo de host en la matriz SAN.

Para obtener información acerca de cómo controlar conflictos de reserva de SCSI en matrices de almacenamiento específico, consulte el artículo de la base de conocimientos de VMware en http://kb.vmware.com/kb/1005009.

Hiperpaginación de rutas de acceso provoca un acceso lento a los LUN

Si el host ESXi no puede acceder a un LUN, o si el acceso es muy lento, es posible que tenga un problema de hiperpaginación de rutas de acceso, también conocido como hiperpaginación de LUN.

Problema

El host no puede acceder a un LUN, o el acceso es muy lento. Los archivos de registro del host podría indicar cambios frecuentes del estado de la ruta de acceso. Por ejemplo:

```
Frequent path state changes are occurring for path vmhba2:C0:T0:L3. This may indicate a
storage problem. Affected device: naa.600600000000000000edd1. Affected datastores: ds1
```

Causa

Este problema podría deberse a la hiperpaginación de las rutas de acceso. La hiperpaginación de rutas de acceso podría ocurrir cuando hay dos hosts que acceden al mismo LUN a través de diferentes procesadores de almacenamiento (SP) y, como resultado, el LUN nunca está disponible.

La hiperpaginación de rutas de acceso suele producirse en matrices activas-pasivas. La hiperpaginación de rutas de acceso también se puede producir en una matriz conectada directamente con conmutación por error de HBA en uno o más nodos. Las matrices activas-activas o las matrices que ofrecen conmutación por error transparente no causan hiperpaginación de rutas de acceso.

Solución

1 Asegúrese de que todos los hosts que comparten el mismo conjunto de LUN en las matrices activas-pasivas usen el mismo procesador de almacenamiento.

2 Corrija cualquier inconsistencia de cableado o máscara entre diferentes hosts y destinos SAN, de manera que todos los HBA vean los mismos destinos.

3 Asegúrese de que las reglas de reclamación en todos los hosts que comparten los LUN sean exactamente iguales.

4 Configure la ruta de acceso para usar la PSP que se utilizó más recientemente, que es la predeterminada.

La mayor latencia para solicitudes de E/S reduce el rendimiento de la máquina virtual

Si el host ESXi genera más comandos hacia un LUN de lo que permite la profundidad de la cola de LUN, el exceso de comandos queda en cola en VMkernel. Esto aumenta la latencia, o el tiempo que se requiere para realizar solicitudes de E/S.

Problema

El host tarda más en realizar las solicitudes de E/S y las máquinas virtuales muestran un rendimiento insatisfactorio.

Causa

El problema podría deberse a una inadecuada profundidad de la cola de LUN. Los controladores de dispositivos SCSI tienen un parámetro configurable llamado Profundidad de la cola de LUN que determina cuántos comandos hacia un LUN determinado pueden estar activos a la vez. Si el host genera más comandos hacia un LUN, el exceso de comandos queda en cola en el VMkernel.

Solución

1 Si la suma de comandos activos de todas las máquinas virtuales excede de forma constante la profundidad del LUN, aumente la profundidad de la cola.

   El procedimiento que se usa para incrementar la profundidad de la cola depende del tipo de adaptador de almacenamiento que usa el host.

2 Cuando hay varias máquinas virtuales activas en un LUN, cambie el parámetro Disk.SchedNumReqOutstanding (DSNRO), para que coincida con el valor de profundidad de la cola.

Ajustar la profundidad de la cola para HBA QLogic, Emulex y Brocade

Si no está satisfecho con el rendimiento de sus adaptadores de bus de hardware (HBA), cambie la profundidad máxima de la cola en su host ESXi.

El valor máximo se refiere a las profundidades de la cola que se informan para diversas rutas de acceso al LUN. Cuando disminuye este valor, acelera la capacidad de proceso del host y las inquietudes de contención del SAN en caso de que haya varios hosts que están utilizando en exceso el almacenamiento y llenando su cola de comandos.

Para ajustar el parámetro de profundidad máxima de la cola, use los comandos vCLI.

En el procedimiento, **`--server=`*`server_name`*** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

1 Compruebe cuál módulo de HBA está cargado actualmente introduciendo el siguiente comando:

```
esxcli --server=server_name system module list | grep module
```

Utilice una de las siguientes opciones para *module*.

Opción	Descripción
qla	QLogic
qln	Controladores nativos de QLogic
lpfc	Emulex
bfa	Brocade

2 Ajuste la profundidad de la cola para el módulo apropiado.

```
esxcli --server=server_name system module parameters set -p
parameter=value -m module
```

Utilice las siguientes cadenas para las opciones *parameter* y *module*.

Cadena	Descripción
-p ql2xmaxqdepth=*value* -m qla2xxx	QLogic
-p ql2xmaxqdepth=*value* -m qlnativefc	Controladores nativos de QLogic
-p lpfc0_lun_queue_depth=*value* -m lpfc820	Emulex

Cadena	Descripción
-p lpfc0_lun_queue_depth=*value* -m lpfc	Controladores nativos de Emulex
-p bfa_lun_queue_depth=*value* -m bfa	Brocade

3 Reinicie el host.

4 Ejecute el siguiente comando para verificar los cambios **esxcli --server=*server_name* system module parameters list -m=*module***.

   module es un controlador apropiado, como **qlnativefc** o **bfa**.

Ajustar la profundidad máxima de la cola para iSCSI de software

Si nota un rendimiento bajo para sus LUN iSCSI de software, cambie la profundidad máxima de la cola ejecutando los comandos `esxcli`.

Requisitos previos

- Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, puede ejecutar comandos `esxcli` en ESXi Shell.
- En el procedimiento, la opción de conexión --server=*server_name* especifica el servidor de destino. Esté preparado para introducir un nombre de usuario y una contraseña cuando el servidor de destino se lo solicite. Para obtener una lista de otras opciones posibles de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Procedimiento

1 Ejecute el siguiente comando:

   esxcli --server=*server_name* system module parameters set -m iscsi_vmk -p iscsivmk_LunQDepth=*value*

   El parámetro `iscsivmk_LunQDepth` establece la cantidad máxima de comandos pendientes, o profundidad de la cola, para cada LUN al que se accede a través del adaptador de iSCSI de software. El valor predeterminado es 128.

2 Reinicie su sistema.

3 Verifique los cambios ejecutando el comando **esxcli --server=*server_name* system module parameters list -m iscsi_vmk**.

   El siguiente resultado muestra la profundidad de la cola para iSCSI de software.

```
iscsivmk_LunQDepth  int   64  Maximum Outstanding Commands Per LUN
```

Resultados

Precaución Si se configura la profundidad de la cola en un valor mayor al predeterminado, se puede reducir la cantidad total de LUN compatibles.

Cambiar la configuración de solicitudes de E/S pendientes

Su ajustó la profundidad de la cola de LUN, cambie el parámetro Disk.SchedNumReqOutstanding (DSNRO), para que su valor coincida con la profundidad de la cola. El parámetro controla la cantidad máxima de solicitudes de E/S pendientes que pueden emitir todas las máquinas virtuales al LUN.

Cambie este parámetro solo cuando tenga varias máquinas virtuales activas en un LUN. El parámetro no se aplica cuando solo hay una máquina virtual activa. En ese caso, el ancho de banda se controla mediante la profundidad de la cola del adaptador de almacenamiento.

El parámetro se configura por dispositivo.

Procedimiento

1 Introduzca el siguiente comando para visualizar la configuración actual de DSNRO para el dispositivo especificado:

   esxcli storage core device list -d *device_ID*

   Se obtiene un resultado similar al siguiente:

   ```
   No of outstanding IOs with competing worlds: 32
   ```

2 Cambie el valor de DSNRO introduciendo el siguiente comando:

   esxcli storage core device set -O | --sched-num-req-outstanding *value* -d *device_ID*

3 Compruebe los cambios introduciendo el siguiente comando:

   esxcli storage core device list -d *device_ID*

Las máquinas virtuales con RDM necesitan ignorar memoria caché de SCSI INQUIRY

Proveedores de almacenamiento podrían requerir que máquinas virtuales con RDM ignoren datos de SCSI INQUIRY almacenados en la memoria caché por ESXi.

Problema

Ciertos sistemas operativos o aplicaciones invitados que se ejecutan en máquinas virtuales con RDM muestran un comportamiento impredecible.

Causa

Este comportamiento podría deberse a que datos de SCSI INQUIRY almacenados en la memoria caché interfieren con sistemas operativos y aplicaciones invitados específicos.

Cuando el host ESXi se conecta por primera vez a un dispositivo de almacenamiento de destino en una SAN, emite el comando SCSI INQUIRY para obtener datos de identificación desde el dispositivo. De forma predeterminada, ESXi almacena en memoria caché los datos de SCSI INQUIRY que se reciben (Estándar, página 80 y página 83) y los datos permanecen sin modificaciones en adelante.

Solución

- Configure la máquina virtual con RDM para ignorar la memoria caché de SCSI INQUIRY agregando el siguiente parámetro al archivo `.vmx`.

  ```
  scsix:y.ignoreDeviceInquiryCache = "true"
  ```

  donde *x* es el número de controladora SCSI y *y* es el número de destino SCSI de RDM.

  Habilite este parámetro únicamente cuando su proveedor de almacenamiento le recomiende que lo haga. Este parámetro es obligatorio solo para una cantidad limitada de matrices de almacenamiento y solo para sistemas operativo invitados específicos.

El adaptador de iSCSI de software está habilitado cuando no es necesario

Cuando el host utiliza un adaptador de red con iBFT, el adaptador de iSCSI de software siempre está activado de forma predeterminada.

Problema

Después del primer arranque del host ESXi, se habilita el adaptador de iSCSI de software y aparece en vSphere Web Client en la lista de adaptadores de almacenamiento.

Causa

El adaptador de red con iBFT habilitado en el host hace que el iSCSI de software siempre esté presente. Esta condición se produce cuando no utiliza iBFT para el arranque de iSCSI.

Solución

Si no emplea el adaptador de red apto con iBFT habilitado para el arranque de iSCSI y no desea que el adaptador de iSCSI de software se habilite, elimine la configuración de iBFT del adaptador de red. Debido a que este proceso es de proveedor específico, consulte la documentación del proveedor para obtener detalles.

Error al montar almacenes de datos de NFS

Los intentos de montar almacenes de datos NFS con nombres en idiomas internacionales producen errores.

Problema

El uso de caracteres no ASCII para nombres de directorios y archivos en el almacenamiento NFS podría provocar un comportamiento impredecible. Por ejemplo, es posible que no pueda montar un almacén de datos NFS ni pueda encender una máquina virtual.

Causa

ESXi admite el uso de caracteres no ASCII para nombres de directorio y archivos en el almacenamiento NFS, por lo que se pueden crear almacenes de datos y máquinas virtuales utilizando nombres en idiomas internacionales. Sin embargo, cuando el servidor NFS subyacente no ofrece compatibilidad de internacionalización, podrían producirse errores impredecibles.

Solución

Siempre asegúrese de que el servidor NFS subyacente ofrezca compatibilidad internacional. Si el servidor no lo hace, solo use caracteres ASCII.

Solucionar problemas de adaptadores de almacenamiento

Si sus adaptadores de almacenamiento experimentan problemas de rendimiento, use los comandos `esxcli storage san` para identificar los problemas.

Problema

Los adaptadores de almacenamiento experimentan problemas de rendimiento y de E/S.

Solución

Use los comandos `esxcli storage san` para obtener y visualizar eventos y estadísticas de los adaptadores. Puede analizar el resultado de los comandos para identificar problemas del adaptador y para buscar las soluciones apropiadas.

Tabla 7-3. comandos de esxcli storage san

<table>
<tr><th>Comando</th><th>Descripción</th><th>Opciones</th></tr>
<tr><td>esxcli storage san fc | iscsi | fcoe | sas list</td><td>Enumera los atributos del adaptador.
Nota iSCSI se aplica solo a iSCSI de software.</td><td>-- adapter | -A
Nombre del adaptador (vmhbaX), o ninguno, para enumerar la información de todos los adaptadores del tipo particular.</td></tr>
<tr><td>esxcli storage san fc | iscsi | fcoe | sas stats get</td><td>Obtiene estadísticas del adaptador.
Nota iSCSI se aplica solo a iSCSI de software.</td><td>-- adapter | -A
Nombre del adaptador (vmhbaX), o ninguno, para enumerar la información de todos los adaptadores del tipo particular.</td></tr>
<tr><td>esxcli storage san fc | fcoe | sas reset</td><td>Restablece un adaptador en particular.</td><td>-- adapter | -A
Nombre del adaptador (vmhbaX).</td></tr>
<tr><td>esxcli storage san fc events get</td><td>Recupera eventos de los adaptadores de canal de fibra.</td><td>-- adapter | -A
Nombre del adaptador (vmhbaX), o ninguno, para enumerar la información de todos los adaptadores de canal de fibra en el sistema.</td></tr>
</table>

Comprobar la coherencia de los metadatos con VOMA

Use vSphere On-disk Metadata Analyzer (VOMA) para identificar incidentes de daños de metadatos que afectan los sistemas de archivos o los volúmenes lógicos subyacentes.

Problema

Cuando experimenta problemas con un almacén de datos de VMFS o un recurso flash virtual, puede revisar la consistencia de los metadatos. Por ejemplo, puede realizar una comprobación de metadatos en los siguientes casos:

- Experimenta interrupciones en el almacenamiento.
- Después de volver a construir RAID o realizar un reemplazo de disco.
- Ve errores de metadatos en el archivo `vmkernel.log` similares a los siguientes:

  ```
  cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402
  ("<Datastore_name>") may be damaged on disk. Corrupt heartbeat detected at offset 3305472:
  [HB state 0 offset 6052837899185946624 gen 15439450 stampUS 5 $
  ```

- No puede tener acceso a archivos en un VMFS.
- Ve que se informa sobre daños para un almacén de datos en las pestañas de eventos de vCenter Server.

Solución

Para comprobar la consistencia de datos, ejecute VOMA en la CLI de un host ESXi. Se puede usar VOMA para comprobar y solucionar problemas menores de inconsistencia de metadatos en un almacén de datos de VMFS o un recurso flash virtual. Para resolver errores que informe VOMA, consulte Soporte de VMware.

Siga estas directrices cuando use la herramienta VOMA:

- Asegúrese de que el almacén de datos de VMFS que analiza no se extienda en múltiples extensiones. Puede ejecutar VOMA solo para un almacén de datos de una sola extensión.
- Apague las máquinas virtuales que estén en ejecución o mígrelas a un almacén de datos diferente.

En el siguiente ejemplo se demuestra cómo usar VOMA para comprobar la consistencia de los metadatos de VMFS.

1 Obtenga el nombre y el número de partición del dispositivo que respalda el almacén de datos de VMFS que quiere revisar.

   #esxcli storage vmfs extent list

   Las columnas Nombre del dispositivo y Partición en el resultado identifican el dispositivo. Por ejemplo:

```
Volume Name  XXXXXXXX  Device Name                             Partition
1TB_VMFS5    XXXXXXXX  naa.00000000000000000000000000000703    3
```

2 Compruebe que no haya errores de VMFS.

   Proporciona una ruta de acceso absoluta a la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS, y entregue un número de partición con el nombre del dispositivo. Por ejemplo:

   # voma -m vmfs -f check -d /vmfs/devices/disks/naa.00000000000000000000000000000703:3

   El resultado enumera posibles errores. Por ejemplo, el siguiente resultado indica que la dirección de latido no es válida.

```
XXXXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
 ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.

Total Errors Found:           1
```

Entre las opciones de comandos que toma la herramienta VOMA se incluyen las siguientes.

Tabla 7-4. Opciones de comandos de VOMA

Opción de comando	Descripción	
`-m|--module`	Los módulos que se ejecutarán incluyen los siguientes:	
	`vmfs`	Si no se especifica el nombre del módulo, se usa esta opción de manera predeterminada. Puede comprobar los sistemas de archivos VMFS y los sistemas de archivos que respaldan los recursos flash virtuales. Si especifica este módulo, también se realizan comprobaciones mínimas para LVM.
	`lvm`	Compruebe los volúmenes lógicos que respaldan los almacenes de datos de VMFS.
	`ptbl`	Comprueba y valida particiones de VMFS, como MBR o GPT. Si no existe ninguna partición, determina si deberían existir particiones.
`-f|--func`	Las funciones que se realizarán incluyen las siguientes:	
	`query`	Enumera funciones compatibles con el módulo.
	`check`	Comprueba errores.
`-d|--device`	Dispositivo o disco que se va a inspeccionar. Asegúrese de proporcionar la ruta de acceso absoluta hacia la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS. Por ejemplo, /vmfs/devices/disks/naa.00000000000000000000000000:1.	
`-s|--logfile`	Especifica el archivo de registro para mostrar los resultados.	
`-v|--version`	Muestra la versión de VOMA.	
`-h|--help`	Muestra el mensaje de ayuda para el comando VOMA.	

Para obtener más información, consulte el artículo 2036767 de la base de conocimientos de VMware.

Ruta de almacenamiento sin conmutación por error cuando el comando TUR arroja un error

La ruta de almacenamiento no conmuta por error cuando el comando TUR devuelve una y otra vez solicitudes de reintento.

Problema

En general, cuando una ruta de almacenamiento experimenta un problema, un host ESXi envía el comando Test Unit Ready (TUR) para confirmar que la ruta está caída antes de iniciar la conmutación por error de la ruta. No obstante, si el comando TUR arroja un error y devuelve una y otra vez una solicitud de operación de reintento (VMK_STORAGE_RETRY_OPERATION),

el host continúa reintentando el comando sin activar la conmutación por error. Normalmente, los siguientes errores provocan que el host reintente el comando TUR:

- SCSI_HOST_BUS_BUSY 0x02
- SCSI_HOST_SOFT_ERROR 0x0b
- SCSI_HOST_RETRY 0x0c

Causa

Para solucionar el problema, puede usar el parámetro `enable|disable_action_OnRetryErrors`. Al habilitar este parámetro, el host ESXi puede marcar la ruta problemática como una ruta caída. Una vez que se marcó la ruta como caída, el host puede activar la conmutación por error y utilizar una ruta alternativa que funcione.

Solución

1 Para establecer el parámetro, ejecute el comando correspondiente:

Acción	Comando
Habilita la capacidad para marcar una ruta problemática como caída.	**`# esxcli storage nmp satp generic deviceconfig set -c enable_action_OnRetryErrors -d naa.XXX`**
Deshabilita la capacidad para marcar una ruta problemática como caída.	**`# esxcli storage nmp satp generic deviceconfig set -c disable_action_OnRetryErrors -d naa.XXX`**

2 Para revisar el estado del parámetro, ejecute el siguiente comando:

`# esxcli storage nmp device list`

El resultado del siguiente ejemplo indica que se habilitó el parámetro:

```
naa.XXX
Device Display Name: DGC Fibre Channel Disk (naa.XXX)
Storage Array Type: VMW_SATP_CX Storage Array Type Device
Config: {navireg ipfilter action_OnRetryErrors}
```

El parámetro `enable|disable_action_OnRetryErrors` es persistente en todos los reinicios.

Solución

También se puede establecer este parámetro al configurar una regla de notificación de SATP:

`# esxcli storage nmp satp rule add -t device -d naa.XXX -s VMW_SATP_EXAMPLE -P VMW_PSP_FIXED -o enable_action_OnRetryErrors`

Solucionar problemas de dispositivos flash

vSphere utiliza unidades flash para funciones de almacenamiento como vSAN, memoria caché de intercambio de host y Flash Read Cache.

Los temas de solución de problemas pueden ayudar a impedir posibles problemas y ofrecen soluciones para problemas que se podrían encontrar al configurar unidades flash.

Los dispositivos flash con formato pueden quedar no disponibles

Un dispositivo local queda no disponible para recurso flash virtual o configuración de Virtual SAN cuando se formatea con VMFS o cualquier otro sistema de archivos.

Problema

Cuando intenta configurar un recurso de vSAN o de flash virtual, no aparece un disco flash local en la lista de discos que se van a usar.

Causa

Este problema se puede producir cuando un disco flash destinado a utilizarse con cualquier función ya se formateó con VMFS. Flash virtual y vSAN no pueden compartir el disco flash con VMFS ni ningún otro sistema de archivos.

Igualmente, debido a que un flash virtual y vSAN son consumidores mutuamente excluyentes de discos flash, ambas características no pueden compartir un disco flash. Si el disco flash ya se reclamó para una característica, por ejemplo vSAN, no puede usarlo para otro, como un flash virtual, a menos que libere el disco.

Solución

Para recurso de flash virtual y configuración de vSAN, use solo discos flash sin formato.

- Evite formatear los discos flash con VMFS durante la instalación de ESXi o Auto Deploy.
- Si el disco flash ya está formateado con VMFS, elimine el almacén de datos de VMFS. Para obtener información, consulte el documento *Almacenamiento de vSphere*.
- Para utilizar el disco flash como recurso de flash virtual, no reclame este disco para vSAN. Si vSAN reclama el disco, quítelo de vSAN. El disco flash se libera de vSAN y queda disponible en la lista de discos para usar con flash virtual. Para obtener información acerca de cómo eliminar discos de vSAN, consulte la documentación de *Administrar VMware vSAN*.
- Si pretende usar el disco flash con vSAN, no utilice el disco para un recurso de flash virtual. Si el disco flash se usa como recurso de flash virtual, elimine la configuración de flash virtual. El disco queda disponible para vSAN. Consulte la documentación de *Almacenamiento de vSphere*.

Otro motivo por el que el disco flash queda no disponible es cuando ESXi no puede detectar el disco. Consulte Discos flash locales están indetectables .

Mantener los discos flash sin VMFS

Si se usa la opción de arranque con creación automática de particiones al instalar o implementar de forma automática ESXi, la opción de partición automática crea un almacén de datos de VMFS en el almacenamiento local del host. En algunos casos, es necesario mantener los discos flash del almacenamiento local sin formato.

Problema

De forma predeterminada, la creación automática de particiones implementa sistemas de archivos de VMFS en cualquier disco de almacenamiento local sin usar en su host, incluidos discos flash.

Sin embargo, un disco flash formateado con VMFS queda no disponible para funciones como disco flash virtual y vSAN. Ambas funciones requieren un disco flash sin formato y tampoco pueden compartir el disco con otro sistema de archivos.

Solución

Para asegurar que la creación automática de particiones no formatee el disco flash con VMFS, use las siguientes opciones de arranque al instalar ESXi o arrancar el host ESXi por primera vez:

- **`autoPartition=TRUE`**
- **`skipPartitioningSsds=TRUE`**

Si utiliza Auto Deploy, configure estos parámetros en un host de referencia.

1. En vSphere Web Client, seleccione el host que planea usar como el host de referencia y haga clic en la pestaña **Configurar**.
2. Haga clic en **Sistema** para abrir las opciones del sistema y haga clic en **Configuración avanzada del sistema**.
3. Desplácese a `VMkernel.Boot.autoPartition` y establezca el valor en true.
4. Desplácese a `VMkernel.Boot.skipPartitioningSsds` y establezca el valor en true.
5. Reinicie el host.

Si los discos flash que planea usar con Flash Read Cache y vSAN ya tienen almacenes de datos de VMFS, elimine los almacenes de datos.

Discos flash locales están indetectables

Si se consultan los discos flash locales, es posible que el host ESXi no devuelva una lista completa de los discos flash locales.

Problema

Es posible que ESXi no pueda detectar los discos flash ni los reconozca como locales. Este problema se puede producir cuando se configuran entidades que solo requieren discos flash locales, por ejemplo, un recurso flash virtual o vSAN.

Causa

ESXi no reconoce ciertos dispositivos como discos flash cuando sus proveedores no admiten detección automática de discos flash. En otros casos, es posible que algunos discos flash no se detecten como locales y ESXi los marque como remotos. Cuando el host no reconoce los discos como discos flash locales, los excluye de la lista de discos disponibles para la configuración.

Solución

Es posible que sea necesario etiquetar los discos como flash o locales.

- Si ESXi no reconoce automáticamente sus discos como discos flash, etiquételos como discos flash.
- Si ESXi no detecta discos flash como locales, configúrelos manualmente como locales.

Marcar dispositivos de almacenamiento como flash

Si ESXi no reconoce los dispositivos como flash, márquelos como dispositivos flash.

ESXi no reconoce ciertos dispositivos como flash cuando los proveedores no admiten la detección automática de discos flash. La columna Tipo de unidad de los dispositivos muestra HDD como el tipo.

Precaución Marcar los dispositivos HDD como flash puede deteriorar el rendimiento de los almacenes de datos y los servicios que los utilizan. Marque los dispositivos únicamente si tiene certeza de que son dispositivos flash.

Requisitos previos

Compruebe que el dispositivo no esté en uso.

Procedimiento

1. Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.
4. En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos HDD para marcarlos como dispositivos flash y haga clic en el icono **Marcar como discos flash** ().
5. Haga clic en **Sí** para guardar los cambios.

Resultados

El tipo de dispositivo cambia a flash.

Pasos siguientes

Si el dispositivo flash que marca se comparte entre varios hosts, asegúrese de marcar el dispositivo en todos los hosts que comparten el dispositivo.

Marcar dispositivos de almacenamiento como locales

ESXi permite marcar dispositivos como locales. Esta acción es útil en los casos en que ESXi no puede determinar si ciertos dispositivos son locales.

Requisitos previos

- Asegúrese de que el dispositivo no esté compartido.

- Apague las máquinas virtuales que residen en ese dispositivo y desmonte los almacenes de datos asociados.

Procedimiento

1. Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
2. Haga clic en la pestaña **Configurar**.
3. En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.
4. En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos remotos para marcarlos como locales y haga clic en el icono **Todas las acciones**.
5. Haga clic en **Marcar como local** y, a continuación, haga clic en **Sí** para guardar los cambios.

Solucionar problemas de Virtual Volumes

Los volúmenes virtuales son encapsulaciones de archivos de máquinas virtuales, discos virtuales y sus derivados. Los volúmenes virtuales se almacenan de manera nativa en un sistema de almacenamiento que está conectado a través de Ethernet o SAN. Un sistema de almacenamiento compatible los exporta como objetos y el hardware los administra completamente en el lado del almacenamiento.

Para obtener información sobre la funcionalidad Virtual Volumes (Volúmenes virtuales), consulte la publicación *Almacenamiento de vSphere*.

Virtual Volumes y comandos esxcli

Puede usar los comandos `esxcli storage vvol` para solucionar problemas para entornos de Virtual Volumes.

Se encuentran disponibles las siguientes opciones de comandos:

Tabla 7-5. Comandos `esxcli storage vvol`

Espacio de nombres	Opción de comando	Descripción
`esxcli storage core device`	`list`	Identifique los endpoints de protocolo. La entrada de resultados `Is VVOL PE: true` indica que el dispositivo de almacenamiento es un endpoint de protocolo.
`esxcli storage vvol daemon`	`unbindall`	Desvincula todos los volúmenes virtuales de todos los proveedores de VASA conocidos para el host ESXi.
`esxcli storage vvol protocolendpoint`	`list`	Enumera todos los extremos del protocolo a los que puede tener acceso su host.

Tabla 7-5. Comandos `esxcli storage vvol` (continuación)

Espacio de nombres	Opción de comando	Descripción
`esxcli storage vvol storagecontainer`	`list` `abandonedvvol scan`	Enumere todos los contenedores de almacenamiento disponibles. Examine el contenedor de almacenamiento especificado en busca de VVol abandonados.
`esxcli storage vvol vasacontext`	`get`	Muestre el contexto de VASA (UUID de VC) asociado al host.
`esxcli storage vvol vasaprovider`	`list`	Enumere todos los proveedores (VASA) de almacenamiento asociados al host.

Un almacén de datos virtual no está accesible

Después de que crea un almacén de datos virtual, queda inaccesible.

Problema

vSphere Web Client muestra que el almacén de datos está inaccesible. No se puede usar el almacén de datos para aprovisionamiento de máquinas virtuales.

Causa

Este problema podría ocurrir cuando no configura los extremos del protocolo para el contenedor de almacenamiento basado en SCSI que está asignado al almacén de datos virtual. Al igual que los LUN tradicionales, los extremos del protocolo SCSI deben configurarse de manera que un host ESXi pueda detectarlos.

Solución

Antes de crear almacenes de datos virtuales para contenedores basados en SCSI, asegúrese de configurar extremos del protocolo en el lado de almacenamiento.

Errores durante la migración de máquinas virtuales o durante la implementación de OVF de máquina virtual en almacenes de datos de Virtual Volumes

Los intentos de migrar una máquina virtual o de implementar una OVF de máquina virtual en almacenes de datos virtuales generan errores.

Problema

Una plantilla de OVF o una máquina virtual que se migra desde un almacén de datos no virtual pueden incluir archivos adicionales de gran tamaño, como imágenes de disco ISO, imágenes de DVD y archivos de imagen. Si estos archivos adicionales hacen que el volumen virtual de

configuración supere su límite de 4 GB, se produce un error en la migración o la implementación en un almacén de datos virtual.

Causa

El volumen virtual de configuración, o config-VVol, contiene varios archivos relacionados con máquinas virtuales. En los almacenes de datos no virtuales tradicionales, estos archivos se almacenan en el directorio principal de la máquina virtual. De forma similar al directorio principal de la máquina virtual, config-VVol incluye el archivo de configuración de máquina virtual, archivos de disco virtual y descriptor de instantáneas, archivos de registro, archivos de bloqueo, etc.

En los almacenes de datos virtuales, todos los demás archivos de gran tamaño, como discos virtuales, instantáneas creadas con memoria, intercambio y resumen, se almacenan en volúmenes virtuales separados.

Los Config-VVols se crean como volúmenes virtuales de 4 GB. El contenido genérico de config-VVol generalmente consume solo una fracción de esta asignación de 4 GB, por lo que los config-VVols casi siempre tienen un aprovisionamiento fino para conservar el espacio de copia de seguridad. Todos los archivos adicionales de gran tamaño, como imágenes de disco ISO, imágenes de DVD y archivos de imagen, pueden hacer que config-VVol supere su límite de 4 GB. Si esos archivos se incluyen en una plantilla de OVF, la implementación de OVF de máquina virtual en el almacenamiento de vSphere Virtual Volumes genera errores. Si esos archivos son parte de una máquina virtual existente, la migración de esa máquina virtual de un almacén de datos tradicional al almacenamiento de vSphere Virtual Volumes también genera errores.

Solución

- Para la migración de máquinas virtuales. Antes de migrar una máquina virtual de un almacén de datos tradicional a un almacén de datos virtual, quite el contenido sobrante del directorio principal de la máquina virtual para que config-VVol no supere el límite de 4 GB.
- Para la implementación de OVF. Ya que no se puede implementar una plantilla de OVF que contenga archivos de más directamente en un almacén de datos virtual, primero se debe implementar la máquina virtual en un almacén de datos no virtual. Quite el contenido de sobra del directorio principal de la máquina virtual y migre esta última al almacenamiento de vSphere Virtual Volumes.

Intentos con errores de migrar máquinas virtuales con instantáneas creadas con memoria a almacenes de datos virtuales y desde ellos

Al intentar migrar una máquina virtual con versión de hardware 10 o anterior a un almacén de datos de vSphere Virtual Volumes o desde él, se producen errores si la máquina virtual tiene instantáneas creadas con memoria.

Problema

Se producen los siguientes problemas cuando se migra una máquina virtual de versión 10 o anterior con instantáneas creadas con memoria:

- La migración de una máquina virtual de versión 10 o anterior con instantáneas creadas con memoria a un almacén de datos virtual no es compatible y produce errores.
- La migración de una máquina virtual de versión 10 o anterior con instantáneas creadas con memoria desde un almacén de datos virtual hacia un almacén de datos no virtual, como VMFS, puede realizarse correctamente. Si posteriormente se crean más instantáneas y se intenta migrar esta máquina virtual al almacenamiento de vSphere Virtual Volumes, se producen errores.

Causa

El almacenamiento de vSphere Virtual Volumes no requiere el uso de una versión de hardware en particular para las máquinas virtuales. Por lo general, es posible trasladar una máquina virtual con cualquier versión de hardware al almacenamiento de vSphere Virtual Volumes. No obstante, si tiene una máquina virtual con instantáneas creadas con memoria y planifica migrarla entre un almacén de datos virtual y un almacén de datos no virtual, utilice una máquina virtual con versión de hardware 11.

Las máquinas virtuales que no sean VVols con versión de hardware 11 o posteriores utilizan archivos diferentes para almacenar sus instantáneas creadas con memoria. Este uso se asemeja a las máquinas virtuales en el almacenamiento de vSphere Virtual Volumes, en que las instantáneas creadas con memoria se originan como VVols distintos en lugar de almacenarse como parte de un archivo `.vmsn` en el directorio de inicio de la máquina virtual. Por el contrario, las máquinas virtuales que no son VVols con versión de hardware 10 continúan almacenando las instantáneas creadas con memoria como parte del archivo `.vmsn` en el directorio de inicio de la máquina virtual. Como resultado, es posible que tenga problemas o se produzcan errores al intentar migrar estas máquinas virtuales entre almacenes de datos virtuales y no virtuales.

Solución

Para evitar problemas al migrar las máquinas virtuales con instantáneas creadas con memoria a través de almacenes de datos virtuales y no virtuales, use la versión de hardware 11. Siga estas instrucciones al migrar máquinas virtuales de versión 10 o anterior con instantáneas creadas con memoria:

- La migración de una máquina virtual de versión 10 o anterior con instantáneas creadas con memoria a un almacén de datos virtual no es compatible. La única solución es quitar todas las instantáneas. La actualización de la versión de hardware no soluciona el problema.
- La migración de una máquina virtual de versión 10 o anterior con instantáneas creadas con memoria desde un almacén de datos virtual hacia un almacén de datos no virtual, como VMFS, puede realizarse correctamente. No obstante, la migración puede colocar a la máquina virtual en un estado incoherente. Las instantáneas tomadas en el almacén de datos virtual

utilizan el objeto `vmem`. Toda instantánea creada con memoria tomada después de migrar a VMFS se almacena en el archivo `.vmsn`. Si, posteriormente, intenta migrar esta máquina virtual al almacenamiento de vSphere Virtual Volumes, se producen errores. Al igual que en el caso anterior, quite todas las instantáneas para solucionar este problema.

Solucionar problemas de filtros de VAIO

vSphere API para los filtros de E/S (VAIO) ofrece un marco que permite que terceros creen componentes de software denominados filtros de E/S. Los filtros pueden instalarse en hosts ESXi y pueden ofrecer servicios de datos adicionales a las máquinas virtuales al procesar solicitudes de E/S que se transfieren entre el sistema operativo invitado de una máquina virtual y los discos virtuales.

Para obtener información sobre los filtros de E/S, consulte la publicación de *Almacenamiento de vSphere*.

Controlar errores de instalación de filtros de E/S

En general, todos los hosts ESXi de un clúster tienen el mismo conjunto de filtros de E/S instalado. En ocasiones, pueden generarse errores durante la instalación.

Si se produce un error en la instalación de un filtro de E/S en un host, el sistema genera eventos que informan acerca del error. Además, una alarma en el host muestra el motivo del error. A continuación se proporcionan ejemplos de errores:

- No se puede obtener acceso a la URL de VIB desde el host.
- El VIB tiene un formato no válido.
- El VIB requiere que el host esté en modo de mantenimiento para ejecutar una actualización o una desinstalación.
- El VIB requiere que el host se reinicie después de ejecutar la instalación o la desinstalación.
- Los intentos para que el host entre en el modo de mantenimiento producen errores porque no se puede evacuar la máquina virtual desde el host.
- El VIB requiere una instalación o una desinstalación manuales.

vCenter Server puede solucionar algunos errores. Es posible que deba intervenir si se generan otros errores. Por ejemplo, es posible que deba editar la URL de VIB, evacuar o apagar las máquinas virtuales de forma manual, o bien instalar o desinstalar los VIB de forma manual.

Instalar filtros de E/S en un único host ESXi

A los fines de solución de problemas, puede descargar un componente de ESXi del filtro de E/S, en un paquete como archivo VIB, e instalarlo en el host ESXi. Utilice el comando `esxcli` para instalar el archivo VIB.

Cuando se especifica un servidor de destino mediante **--server=server_name**, el servidor le solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface* o ejecute `esxcli --help` en el símbolo del sistema de vCLI.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

1 Instale VIB al ejecutar el siguiente comando:

   ```
   esxcli --server=server_name software vib install --depot
   path_to_VMware_vib_ZIP_file
   ```

   Las opciones del comando `install` permiten realizar un simulacro, especificar un VIB, omitir la comprobación del nivel de aceptación, etc. No omita la comprobación en los sistemas de producción. Consulte la documentación de *Referencia de vSphere Command-Line Interface*.

2 Compruebe que los VIB estén instalados en el host ESXi.

   ```
   esxcli --server=server_name software vib list
   ```

Solucionar problemas de redes

8

Los temas de solución de problemas sobre redes en vSphere ofrecen soluciones a posibles problemas que podrían encontrarse con la conectividad de hosts ESXi, vCenter Server y máquinas virtuales.

Este capítulo incluye los siguientes temas:

Solucionar problemas de asignación de direcciones MAC

En vSphere, ciertas restricciones en el rango de direcciones MAC que se pueden asignar a máquinas virtuales podrían provocar pérdida de conectividad o incapacidad de encender cargas de trabajo.

Duplicar direcciones MAC de máquinas virtuales en la misma red

Se puede encontrar pérdida de paquetes y conectividad debido a que las máquinas virtuales tienen direcciones MAC duplicadas que generó vCenter Server.

Problema

Las direcciones MAC de las máquinas virtuales en el mismo dominio de difusión o subred IP están en conflicto o vCenter Server genera una dirección MAC duplicada para una máquina virtual creada recientemente.

Una máquina virtual se enciende y funciona adecuadamente, pero comparte una dirección MAC con otras máquinas virtuales. Esta situación podría provocar pérdida de paquetes y otros problemas.

Causa

Las máquinas virtuales tienen direcciones MAC duplicadas debido a varios motivos.

- Dos instancias de vCenter Server con identificadores idénticos generan superposición de direcciones MAC para adaptadores de red de máquina virtual.

  Cada instancia de vCenter Server tiene un identificador entre 0 y 63 que se genera de forma aleatoria en el momento de la instalación, pero puede volver a configurarse después de la instalación. vCenter Server utiliza el identificador de la instancia para generar direcciones MAC para los adaptadores de red de la máquina.

- Una máquina virtual se ha transferido en estado apagado desde una instancia de vCenter Server hacia otra en la misma red, por ejemplo, mediante el uso de almacenamiento compartido, y un adaptador de red de la nueva máquina virtual en el primer vCenter Server recibe la dirección MAC liberada.

Solución

◆ Cambie manualmente la dirección MAC de un adaptador de red de máquina virtual.

  Si tiene una máquina virtual existente con una dirección MAC en conflicto, debe proporcionar una dirección MAC única en la configuración **Hardware virtual**.

  - Apague la máquina virtual, configure el adaptador para que utilice una dirección MAC manual y escriba la nueva dirección.
  - Si no puede apagar la máquina virtual para configurarla, vuelva a crear el adaptador de red que está en conflicto con la opción habilitada para asignación manual de dirección MAC y escriba la nueva dirección. En el sistema operativo invitado, configure la misma dirección IP estática que antes para el adaptador que se volvió a agregar.

Para obtener información acerca de cómo configurar los adaptadores de red de máquinas virtuales, consulte la documentación de *Redes de vSphere* y *Administrar máquinas virtuales de vSphere*.

- Si la instancia de vCenter Server genera las direcciones MAC de las máquinas virtuales de acuerdo con la asignación predeterminada, VMware OUI, cambie el identificador de la instancia de vCenter Server o use otro método de asignación para resolver conflictos.

  Nota El cambio del identificador de la instancia de vCenter Server o el cambio a un esquema de asignación diferente no resuelve los conflictos de dirección MAC en máquinas virtuales existentes. Solo las máquinas virtuales creadas o adaptadores de red agregados después del cambio reciben direcciones de acuerdo con el nuevo esquema.

Para obtener información acerca de los esquemas de asignación e instalación de direcciones MAC, consulte la documentación de *Redes de vSphere*.

Solución	Descripción
Cambio del identificador de vCenter Server	Puede mantener el esquema de asignaciones de VMware OUI si su implementación contiene una pequeña cantidad de instancias de vCenter Server. De acuerdo con este esquema, una dirección MAC tiene el siguiente formato: `00:50:56:XX:YY:ZZ` donde `00:50:56` representa VMware OUI, *XX* se calcula como (80 + identificador de vCenter Server) e *YY:ZZ* es un número aleatorio. Para cambiar el identificador de vCenter Server, configure la opción **Identificador único de vCenter Server** en la sección **Tiempo de ejecución** en la configuración **General** de la instancia de vCenter Server y reiníciela. La asignación de VMware OUI funciona con hasta 64 instancias de vCenter Server y es adecuada para implementaciones de pequeña escala.
Cambio a asignación basada en prefijo	Puede usar un OUI personalizado. Por ejemplo, para un rango administrado de forma local `02:12:34`, las direcciones MAC tienen el formato `02:12:34:XX:YY:ZZ`. Puede utilizar el cuarto octeto *XX* para distribuir el espacio de direcciones de OUI entre las instancias de vCenter Server. Esta estructura da como resultado 255 clústeres de direcciones, donde a cada clúster lo administra una instancia de vCenter Server, y aproximadamente 65.000 direcciones MAC por vCenter Server. Por ejemplo, `02:12:34:01:YY:ZZ` para vCenter Server A, `02:12:34:02:YY:ZZ` para vCenter Server B, etc. La asignación basada en prefijo es adecuada para implementaciones de mayor escala. Para direcciones MAC globalmente únicas, el OUI debe estar registrado en el IEEE.

a Configure la asignación de direcciones MAC.

b Aplique el nuevo esquema de asignación de direcciones MAC a una máquina virtual existente en su configuración de **Hardware virtual**.

- Apague una máquina virtual, configure el adaptador para usar una dirección MAC manual, revierta a asignación de direcciones MAC automática y encienda la máquina virtual.
- Si la máquina virtual está en producción y no puede apagarla para realizar configuración, después de cambiar el identificador o el esquema de asignación de direcciones de vCenter Server, vuelva a crear el adaptador de red en conflicto con asignación automática de direcciones MAC habilitada. En el sistema operativo invitado, configure la misma dirección IP estática que antes para el adaptador que se volvió a agregar.

- Aplique la regeneración de direcciones MAC cuando transfiera una máquina virtual entre instancias devCenter Server mediante el uso de los archivos de la máquina virtual desde un almacén de datos.

  a Apague una máquina virtual, sáquela del inventario y, en su archivo de configuración (`.vmx`), configure el parámetro `ethernetX.addressType` a **`generado`**.

  `X` junto a `ethernet` representa el número de secuencia de la NIC virtual en la máquina virtual.

  b Importe la máquina virtual desde un sistema de vCenter Server a otro mediante el registro de la máquina virtual desde un almacén de datos en vCenter Server de destino.

  Los archivos de máquinas virtuales pueden residir en un almacén de datos que se comparte entre las dos instancias devCenter Server o pueden cargarse a un almacén de datos al que se puede acceder desde el sistema de vCenter Server de destino.

  Para obtener información sobre cómo registrar una máquina virtual desde un almacén de datos, consulte *Administrar máquinas virtuales de vSphere*.

  c Encienda las máquinas virtuales por primera vez.

  Mientras la máquina virtual arranca, aparece un icono de información en la máquina virtual en vSphere Web Client.

  d Haga clic con el botón derecho en la máquina virtual y seleccione **Sistema operativo invitado > Responder pregunta**.

  e Seleccione la opción **Lo copié**.

  vCenter Server de destino vuelve a generar la dirección MAC de la máquina virtual. La nueva dirección MAC comienza con el VMware OUI `00:0c:29` y está basada en el UUID del BIOS de la máquina virtual. El UUID del BIOS de la máquina virtual se calcula a partir del UUID del BIOS del host.

- Si vCenter Server y los hosts son de la versión 6.0 y posteriores y las instancias de vCenter Server están conectadas en Enhanced Linked Mode, migre las máquinas virtuales usando vMotion entre sistemas de vCenter Server.

  Cuando se migra una máquina virtual entre sistemas de vCenter Server, vCenter Server de origen agrega la dirección MAC de la máquina virtual a una lista de no permitidos y no la asigna a otras máquinas virtuales.

Error al intentar encender una máquina virtual debido a un conflicto de dirección MAC

Después de configurar cierta dirección MAC estática para un adaptador de máquina virtual, no puede encender la máquina virtual.

Problema

En vSphere Web Client, después de asignar una dirección MAC a una máquina virtual en el rango `00:50:56:40:YY:ZZ` – `00:50:56:7F:YY:ZZ`, se produce error al intentar encender la máquina virtual con un mensaje de estado que indica que la dirección MAC está en conflicto.

```
00:50:56:XX:YY:ZZ no es una dirección Ethernet estática válida. Está en conflicto con las MAC
reservadas de VMware para otros usos.
```

Causa

Intenta asignar una dirección MAC que comienza con VMware OUI `00:50:56` y se encuentra dentro del rango de dirección asignado para adaptadores de VMkernel para host en el sistema de vCenter Server.

Solución

Si desea mantener el prefijo OUI de VMware, configure una dirección MAC estática dentro del rango `00:50:56:00:00:00` – `00:50:56:3F:FF:FF`. De lo contrario, configure una dirección MAC arbitraria cuyo prefijo es diferente del OUI de VMware. Para obtener información sobre los rangos disponibles para direcciones MAC estáticas que tienen el prefijo OUI de VMware, consulte la documentación de *Redes de vSphere*.

Error en la conversión a la compatibilidad de LACP mejorado

Bajo ciertas condiciones, es posible que se produzcan errores en la conversión de una configuración de LACP existente a la compatibilidad de LACP mejorado en una instancia de vSphere Distributed Switch 5.5 y versiones posteriores.

Problema

Después de actualizar vSphere Distributed Switch a la versión 5.5 y posterior, cuando inicia la conversión a la compatibilidad de LACP mejorado a partir de una configuración de LACP existente, se producen errores en la conversión en cierta etapa del proceso.

Causa

La conversión de una configuración de LACP existente a la compatibilidad de LACP mejorado incluye varias tareas para volver a configurar el conmutador distribuido. La conversión podría generar errores debido a que otro usuario puede volver a configurar el conmutador distribuido durante la conversión. Por ejemplo, las NIC físicas de los hosts podrían haberse reasignado a diferentes vínculos superiores o es posible que haya cambiado la configuración de formación de equipos o conmutación por error de los grupos de puertos distribuidos.

El error también podría haber sido causado por la desconexión de algunos hosts durante la conversión.

Solución

Cuando la conversión a la compatibilidad de LACP mejorado genera errores en cierta etapa, se realiza solo parcialmente. Debe comprobar la configuración del conmutador distribuido y los hosts participantes para identificar los objetos con configuración de LACP incompleta.

Compruebe que la configuración de destino que debe resultar de cada etapa de conversión esté en el orden que se indica en la tabla. Cuando localice la etapa donde se produjo el error de conversión, concluya la configuración de destino manualmente y continúe con las siguientes etapas.

Tabla 8-1. Pasos para realizar la conversión manual al LACP mejorado

Etapa de conversión	Estado de la configuración de destino	Solución
1. Cree un nuevo LAG.	Debe haber presente un LAG creado recientemente en el conmutador distribuido.	Compruebe la configuración del LACP del conmutador distribuido y cree un nuevo LAG si no hay ninguno.
2. Cree una configuración intermedia de formación de equipos y conmutación por error de LACP en los grupos de puertos distribuidos.	El LAG creado recientemente debe estar en espera que le permita migrar NIC físicas al LAG sin perder conectividad.	Compruebe la configuración de formación de equipos y conmutación por error del grupo de puertos distribuidos. Configure el nuevo LAG en espera en caso de que no lo esté. Si no desea usar un LAG para que controle el tráfico para todos los grupos de puertos distribuidos, revierta la configuración de formación de equipos y conmutación por error a un estado donde hay vínculos superiores independientes activos y el LAG está sin usar.
3. Reasigne NIC físicas desde vínculos superiores independientes a puertos de LAG.	Todas las NIC físicas de los puertos de LAG deben volver a asignarse desde vínculos superiores independientes a los puertos de LAG	Compruebe si las NIC físicas están asignadas a los puertos de LAG. Asigne una NIC física a cada puerto de LAG. **Nota** El LAG debe permanecer en espera en el orden de formación de equipos y conmutación por error de los grupos de puertos distribuidos mientras vuelve a asignar NIC físicas a los puertos de LAG.
4. Cree la configuración final de formación de equipos y conmutación por error de LACP en los grupos de puertos distribuidos.	La configuración final de formación de equipos y conmutación por error de LACP es la siguiente. ■ Active (Activa): solo el nuevo LAG ■ Standby (En espera): vacíos ■ Unused (Sin utilizar): todos los vínculos superiores independientes	Compruebe la configuración de formación de equipos y conmutación por error del grupo de puertos distribuidos. Cree una configuración válida de formación de equipos y conmutación por error de LACP para todos los grupos de puertos distribuidos a los que desea aplicar LACP.

Ejemplo

Por ejemplo, suponga que verifica que se creó un nuevo LAG en el conmutador distribuido y que se creó una configuración intermedia de formación de equipos y conmutación por error para los grupos de puertos distribuidos. Continúa con la comprobación para determinar si hay NIC físicas asignadas a los puertos de LAG. Descubre que no todos los hosts tienen NIC físicas asignadas a los puertos de LAG, y asigna las NIC manualmente. Concluye la conversión creando la configuración final de formación de equipos y conmutación por error de LACP para los grupos de puertos distribuidos.

No es posible eliminar un host de vSphere Distributed Switch

En ciertas condiciones, es posible que no pueda eliminar un host de vSphere Distributed Switch.

Problema

- Hay error en los intentos por eliminar un host de vSphere Distributed Switch, y recibe una notificación de que los recursos siguen en uso. La notificación que recibe podría verse de la siguiente manera:

  ```
  The resource '16' is in use. vDS DSwitch port 16 is still on host 10.23.112.2 connected to
  MyVM nic=4000 type=vmVnic
  ```

- Hubo error en los intentos de eliminar un conmutador proxy de host que aún existe en el host de una configuración de redes anterior. Por ejemplo, movió el host a un centro de datos diferente o sistema de vCenter Server o actualizó el software deESXi y vCenter Server y creó nueva configuración de redes. Cuando se intenta eliminar el conmutador proxy del host, hay error en la operación, ya que los recursos en el conmutador del proxy siguen en uso.

Causa

No puede quitar el host del conmutador distribuido o eliminar el conmutador proxy del host debido a los siguientes motivos.

- Hay adaptadores de VMkernel en el conmutador que están en uso.
- Existen adaptadores de red de máquina virtual conectados al conmutador.

Solución

Problema	Solución
No se puede eliminar un host de un conmutador distribuido	1 En vSphere Web Client, desplácese hasta el conmutador distribuido. 2 En la pestaña **Configurar**, seleccione **Más > Puertos**. 3 Ubique todos los puertos que siguen en uso y compruebe cuáles adaptadores de red de VMkernel o de máquina virtual en el host siguen conectados a los puertos. 4 Migre o elimine los adaptadores de red de VMkernel y de máquina virtual que sigan conectados al conmutador. 5 Use el asistente **Agregar y administrar hosts** en vSphere Web Client para eliminar el host del conmutador. Después de que se quita el host, el conmutador proxy del host se elimina automáticamente.
No se puede eliminar un conmutador proxy del host	1 En vSphere Web Client, desplácese hasta el host. 2 Elimine o migre los adaptadores de red de VMkernel o de máquina virtual que sigan conectados al conmutador proxy del host. 3 Elimine el conmutador proxy del host de la vista Redes en el host.

Los hosts en vSphere Distributed Switch 5.1 y versiones posteriores pierden conectividad con vCenter Server

Los hosts en vSphere Distributed Switch 5.1 y versiones posteriores no pueden conectarse a vCenter Server después de la configuración de un grupo de puertos.

Problema

Después de cambiar la configuración de redes de un grupo de puertos en vSphere Distributed Switch 5.1 y versiones posteriores que contienen los adaptadores de VMkernel para la red de administración, los hosts en el conmutador pierden conectividad con vCenter Server. En vSphere Web Client el estado de los hosts no tiene capacidad de respuesta.

Causa

En vSphere Distributed Switch 5.1 y versiones posteriores en vCenter Server que tienen reversión de redes deshabilitada, el grupo de puertos que contiene los adaptadores de VMkernel para la red de administración está mal configurado en vCenter Server y la configuración inválida se propaga a los hosts en el conmutador.

Nota En vSphere 5.1 y versiones posteriores, la reversión de redes está habilitada de forma predeterminada. Sin embargo, puede habilitar o deshabilitar las reversiones en el nivel de vCenter Server. Para obtener más información, consulte la documentación *Redes de vSphere*.

Solución

1 Desde la interfaz de usuario de la consola directa (DCUI) hacia un host afectado, use la opción **Restaurar vDS** en el menú **Opciones de restauración de la red** para configurar los vínculos superiores y el identificador de la VLAN para la red de administración.

   La DCUI crea un puerto efímero local y aplica la configuración de la VLAN y del vínculo superior al puerto. La DCUI cambia el adaptador de VMkernel para la red de administración a fin de usar el nuevo puerto local del host para restaurar la conectividad con vCenter Server.

   Después de que el host se vuelve a conectar a vCenter Server, vSphere Web Client muestra una advertencia de que algunos hosts en el conmutador tienen una configuración de redes diferente respecto de la configuración almacenada en vSphere Distributed Switch.

2 En vSphere Web Client, configure el grupo de puertos distribuidos para la red de administración con la configuración correcta.

Situación	Solución
Ha alterado la configuración del grupo de puertos solo una vez	Puede revertir la configuración del grupo de puertos un paso atrás. Haga clic con el botón derecho en el grupo de puertos, luego haga clic en **Restaurar configuración** y seleccione **Restaurar a configuración anterior**.
Ha realizado copia de seguridad de una configuración válida del grupo de puertos	Puede restaurar la configuración del grupo de puertos usando el archivo de copia de seguridad. Haga clic con el botón derecho en el grupo de puertos, luego haga clic en **Restaurar configuración** y seleccione **Restaurar configuración de un archivo**. También puede restaurar la configuración para el conmutador completo, incluido el grupo de puertos, desde un archivo de copia de seguridad para el conmutador.
Ha realizado más de un paso de configuración y no tiene un archivo de copia de seguridad	Debe proporcionar manualmente una configuración válida para el grupo de puertos.

   Para obtener información acerca de la reversión de redes, la recuperación y la restauración, consulte la documentación de *Redes de vSphere*.

3 Migre el adaptador de VMkernel para la red de administración desde el puerto efímero local del host hacia un puerto distribuido en el conmutador mediante el uso del asistente **Agregar y administrar hosts**.

   A diferencia de los puertos distribuidos, el puerto local efímero del VMKernel tiene un identificador que no es numérico.

   Para obtener información sobre cómo controlar adaptadores de VMkernel a través del asistente **Agregar y administrar hosts**, consulte la documentación de *Redes de vSphere*.

4 Aplique la configuración del grupo de puertos distribuido y el adaptador de VMkernel desde vCenter Server hacia el host.

   - Inserte la configuración correcta del grupo de puertos distribuidos y el adaptador de VMkernel devCenter Server en el host.

     a En vSphere Web Client, desplácese hasta el host.

b En la pestaña **Configurar**, haga clic en **Redes**.

c En la lista **Conmutadores virtuales**, seleccione el conmutador distribuido y haga clic en **Rectificar el estado del Distributed Switch seleccionado en el host**.

- Espere hasta que vCenter Server aplique la configuración en las próximas 24 horas.

Los hosts en vSphere Distributed Switch 5.0 y versiones anteriores pierden conectividad con vCenter Server

Los hosts en vSphere Distributed Switch 5.0 y versiones anteriores no pueden conectarse a vCenter Server después de la configuración de un grupo de puertos.

Problema

Después de cambiar la configuración de redes de un grupo de puertos en vSphere Distributed Switch 5.0 o versiones anteriores que contienen los adaptadores de VMkernel para la red de administración, los hosts en el conmutador pierden conectividad con vCenter Server. En vSphere Web Client el estado de los hosts no tiene capacidad de respuesta.

Causa

En vSphere Distributed Switch 5.0 y versiones anteriores en vCenter Server, el grupo de puertos que contiene los adaptadores de VMkernel para la red de administración está mal configurado en vCenter Server y la configuración inválida se propaga a los hosts en el conmutador.

Solución

1 Conecte con un host afectado mediante el uso de vSphere Client.

2 En **Configuración**, seleccione**Redes**.

3 En la vista Conmutador estándar de vSphere, cree un nuevo conmutador estándar si el host no tiene un conmutador estándar adecuado para la red de administración.

   a Haga clic en **Agregar redes**.

   b En el asistente **Agregar red**, en Tipos de conexión escoja **Máquina virtual** y haga clic en **Siguiente**.

   c Seleccione **Crear un conmutador estándar de vSphere**.

   d En la sección **Crear un conmutador estándar de vSphere**, seleccione uno o más adaptadores físicos sin ocupar en el host para realizar el tráfico de administración y haga clic en **Siguiente**.

   Si todos los adaptadores físicos ya están ocupados con tráfico de otros conmutadores, cree el conmutador sin un adaptador de red físico conectado. Posteriormente, quite el adaptador físico de la red de administración desde el conmutador proxy del conmutador distribuido y agréguelo a este conmutador estándar.

e En la sección Propiedades del grupo de puertos, escriba una etiqueta de red que identifique el grupo de puertos que está creando y, opcionalmente, un identificador de VLAN.

f Haga clic en **Finalizar**.

4 Change to: En la vista vSphere Distributed Switch, migre el adaptador de VMkernel para la red a un conmutador estándar.

   a Seleccione la vista vSphere Distributed Switch, y para el conmutador distribuido, haga clic en **Administrar adaptadores virtuales**.

   b En el asistente **Administrar adaptadores virtuales**, seleccione el adaptador de VMkernel de la lista y haga clic en **Migrar**.

   c Seleccione el conmutador estándar creado recientemente u otro al cual migrar el adaptador y haga clic en **Siguiente**.

   d Introduzca una etiqueta de red que sea única en el ámbito del host y, opcionalmente, un identificador de VLAN para la red de administración y haga clic en **Siguiente**.

   e Revise la configuración en el conmutador estándar de destino y haga clic en **Finalizar**.

5 En vSphere Web Client, configure el grupo de puertos distribuidos para la red de administración con la configuración correcta.

6 Migre el adaptador de VMkernel para la red de administración desde el conmutador estándar a un puerto en el conmutador distribuido mediante el uso del asistente **Agregar y administrar hosts**.

   Para obtener información acerca del asistente **Agregar y administrar hosts**, consulte la documentación de *Redes de vSphere*.

7 Si ha movido el adaptador físico desde el conmutador proxy hacia el conmutador estándar, puede volver a conectarlo al conmutador distribuido usando el asistente **Agregar y administrar hosts**.

Alarma de pérdida de redundancia de red en un host

Una alarma informa de una pérdida de redundancia de vínculo superior en un conmutador estándar o distribuido de vSphere para un host.

Problema

No hay NIC físicas redundantes para un host que estén conectadas a un conmutador estándar o distribuido en particular, y aparece la siguiente alarma:

```
Host name or IP Network uplink redundancy lost
```

Causa

Solo una NIC física en el host está conectada a cierto conmutador estándar o distribuido. Las NIC físicas redundantes están caídas o no están asignadas al conmutador.

Por ejemplo, suponga que un host en su entorno tiene NIC físicas *vmnic0* y *vmnic1* conectadas a*vSwitch0*, y la NIC física *vmnic1* queda sin conexión, lo que deja solo a*vmnic0* conectada a *vSwitch0*. Como resultado, la redundancia del vínculo superior para *vSwitch0* se pierde en el host.

Solución

Compruebe cuál switch ha perdido redundancia de vínculo superior en el host. Conecte al menos una NIC física más en el host a este conmutados y restablezca la alarma para que quede en verde. Puede usar vSphere Web Client o ESXi Shell.

Si una NIC física está caída, pruebe colocarla en línea nuevamente mediante el uso deESXi Shell en el host.

Para obtener información sobre el uso de los comandos de redes en ESXi Shell, consulte *Referencia de vSphere Command-Line Interface*. Para obtener información sobre cómo configurar redes en un host en vSphere Web Client, consulte *Redes de vSphere*.

Las máquinas virtuales pierden conectividad después de cambiar el orden de conmutación por error de vínculos superiores de un grupo de puertos distribuidos

Los cambios en el orden de NIC de conmutación por error en un grupo de puertos distribuidos hacen que las máquinas virtuales asociadas con el grupo se desconecten de la red externa.

Problema

Después de que vuelve a disponer los vínculos superiores en los grupos de conmutación por error para un grupo de puertos distribuidos en vCenter Server, por ejemplo, usando vSphere Web Client, algunas máquinas virtuales en el grupo de puertos ya no pueden acceder a la red externa.

Causa

Después de cambiar el orden de conmutación por error, por muchos motivos las máquinas virtuales podrían perder conectividad con la red externa.

- El host que ejecuta las máquinas virtuales no tiene NIC físicas asociadas con los vínculos superiores que están configurados como activos o en espera. Todos los vínculos superiores que están asociados con NIC físicas del host para el grupo de puertos se mueven a sin utilizar.
- Un grupo de agregación de vínculos (LAG) que no tiene NIC físicas desde el host está configurado como el único vínculo superior activo de acuerdo con los requisitos para usar LACP en vSphere.

- Si el tráfico de la máquina virtual está separado en VLAN, los adaptadores físicos del host para los vínculos superiores activos podrían conectarse a puertos de troncal en el conmutador físico que no controla tráfico desde estas VLAN.
- Si el grupo de puertos está configurado con directiva de equilibrio de carga con hash de IP, se conecta un adaptador de vínculo superior activo a un puerto de conmutador físico que puede que no esté en un EtherChannel.

Puede analizar la conectividad de las máquinas virtuales en el grupo de puertos a los vínculos superiores del host y los adaptadores de vínculos superiores asociados desde el diagrama de topología central del conmutador distribuido o desde el diagrama de conmutador de proxy para el host.

Solución

- ◆ Restaure el orden de conmutación por error con el vínculo superior que está asociado con una sola NIC física en el host que vuelve a estar activo.
- ◆ Cree un grupo de puertos con configuración idéntica, asegúrese de usar el número de vínculo superior válido para el host y migre las redes de la máquina virtual hacia el grupo de puertos.
- ◆ Mueva la NIC a un vínculo superior que participa en el grupo de conmutación por error activo.

  Puede usar vSphere Web Client para mover la NIC física del host a otro vínculo superior.

  - Use el asistente **Agregar y administrar hosts** en el conmutador distribuido.
    a. Desplácese al conmutador distribuido en vSphere Web Client.
    b. En el menú **Acciones**, seleccione **Agregar y administrar hosts**.
    c. En la página **Seleccionar tarea**, seleccione la opción **Administrar redes de host** y seleccione el host.
    d. Para asignar la NIC del host a un vínculo superior activo, desplácese hasta la página **Administrar adaptadores de red físicos** y asocie la NIC al vínculo superior del conmutador.
  - Mueva la NIC al nivel del host.
    a. Desplácese hasta el host en vSphere Web Client, y en la pestaña **Configurar**, expanda el menú **Redes**.
    b. Seleccione **Conmutadores virtuales** y escoja el conmutador de proxy distribuido.
    c. Haga clic en **Administrar adaptadores de red físicos conectados al conmutador seleccionado** y mueva la NIC hacia el vínculo superior activo.

No se puede agregar un adaptador físico a vSphere Distributed Switch que tiene Network I/O Control habilitado

Puede que no sea capaz de agregar un adaptador físico con baja velocidad, por ejemplo 1 Gbps, a una instancia de vSphere Distributed Switch que tenga configurado vSphere Network I/O Control versión 3.

Problema

Intenta agregar un adaptador físico con baja velocidad, por ejemplo,1 Gbps, a una instancia de vSphere Distributed Switch que está conectado a adaptadores físicos con alta velocidad, como 10 Gbps. Network I/O Control versión 3 está habilitado en el conmutador y existen reservas de ancho de banda para uno o más tipos de tráfico del sistema, como tráfico de administración de vSphere, tráfico de vSphere vMotion, tráfico de NFS de vSphere NFS, etc. La tarea de agregar el adaptador físico genera errores con un mensaje de estado de que hay un parámetro incorrecto.

```
Un parámetro especificado no era correcto: spec.host[].backing.pnicSpec[]
```

Causa

Network I/O Control alinea el ancho de banda que está disponible para reserva con la velocidad de 10 Gbps de los adaptadores físicos individuales que ya están conectados al conmutador distribuido. Después de que reserva parte de este ancho de banda, puede que si se agrega un adaptador físico cuya velocidad sea menor a 10 Gbps no se satisfagan las potenciales necesidades de un tipo de tráfico del sistema.

Para obtener información sobre Network I/O Control versión 3, consulte la documentación de *Redes de vSphere*.

Solución

1 En vSphere Web Client, desplácese hasta el host.

2 En la pestaña **Configurar**, expanda el grupo de configuración **Sistema**.

3 Seleccione **Configuración avanzada del sistema** y haga clic en **Editar**.

4 Escriba una lista de los adaptadores físicos que desea usar fuera del ámbito de Network I/O Control separados por comas para el parámetro `Net.IOControlPnicOptOut`.

   Por ejemplo: **`vmnic2,vmnic3`**

5 Haga clic en **Aceptar** para aplicar los cambios.

6 En vSphere Web Client, agregue el adaptador físico al conmutador distribuido.

Solucionar problemas de cargas de trabajo con SR-IOV habilitado

En ciertas condiciones, es posible que se experimenten problemas de conectividad o encendido con máquinas virtuales que usan SR-IOV para enviar datos a adaptadores de red físicos.

La carga de trabajo con SR-IOV habilitado no puede comunicarse después de que cambia su dirección MAC

Después de que cambie la dirección MAC en el sistema operativo invitado de una máquina virtual con SR-IOV habilitado, dicha máquina pierde conectividad.

Problema

Cuando conecta el adaptador de red de una máquina virtual a una función virtual (VF) de SR-IOV, crea un adaptador de red de acceso directo para la máquina virtual. Después de que el controlador de VF en el sistema operativo invitado modifica la dirección MAC para el adaptador de red de acceso directo, el sistema operativo invitado muestra que el cambio es correcto, pero que el adaptador de red de la máquina virtual pierde conectividad. Aunque el sistema operativo invitado muestra que la dirección MAC está habilitada, un mensaje de registro en el archivo `/var/log/vmkernel.log` indica que hubo error en la operación.

```
Requested mac address change to new MAC address on port VM NIC port number, disallowed by
vswitch policy.
```

donde

- *new MAC address* es la dirección MAC en el sistema operativo invitado.
- *VM NIC port number* es el número de puerto del adaptador de red de la máquina virtual; en formato hexadecimal.

Causa

La directiva de seguridad predeterminada en el grupo de puertos al cual se conecta el adaptador de red de acceso directo no permite cambios en la dirección MAC en el sistema operativo invitado. Como resultado, la interfaz de redes en el sistema operativo invitado no puede adquirir una dirección IP y pierde conectividad.

Solución

- En el sistema operativo invitado, restablezca la interfaz para que el adaptador de red de acceso directo vuelva a tener su dirección MAC válida. Si la interfaz está configurada para que utilice DHCP para asignación de direcciones, la interfaz adquiere una dirección IP de forma automática.

  Por ejemplo, en una máquina virtual Linux, ejecute el comando de consola `ifconfig`.

  ```
  ifconfig ethX down
  ifconfig ethX up
  ```

donde *X* en `ethX` representa el número de secuencia del adaptador de red de máquina virtual en el sistema operativo invitado.

Una máquina virtual que ejecuta un cliente de VPN provoca una denegación de servicio para máquinas virtuales en el host o a través de un clúster de vSphere HA

Una máquina virtual que envía tramas de Bridge Protocol Data Unit (BPDU), por ejemplo, a un cliente de VPN, hace que algunas máquinas virtuales conectadas al mismo grupo de puertos pierdan conectividad. La transmisión de tramas de BPDU también podría interrumpir la conexión del host o el clúster de vSphere HA primario.

Problema

Una máquina virtual que se espera que envíe tramas de BPDU hace que se bloquee el tráfico hacia la red externa de las máquinas virtuales en el mismo grupo de puertos.

Si la máquina virtual se ejecuta en un host que forma parte de un clúster de vSphere HA, y el host queda aislado de la red bajo ciertas condiciones, observa una denegación de servicio (DoS) en los hosts en el clúster.

Causa

Una práctica recomendada es que un puerto de un conmutador físico se conecte a un host ESXi que tenga la protección Port Fast y BPDU habilitada para aplicar el límite del protocolo de árbol de expansión (Spanning Tree Protocol, STP). Un conmutador estándar o distribuido no es compatible con STP y no envía tramas de BPDU al puerto del conmutador. Sin embargo, si alguna trama de BPDU desde una máquina virtual en riesgo llega a un puerto de un conmutador físico que apunta a un host ESXi, la característica de protección de BPDU deshabilita el puerto para que se detengan las tramas que afectan la topología de árbol de expansión de la red.

En ciertos casos, se espera que una máquina virtual envíe tramas de BPDU, por ejemplo, cuando se implementa una VPN que está conectada a través de un dispositivo puente de Windows o a través de una función de puente. Si el puerto del conmutador físico emparejado con el adaptador físico que controla el tráfico desde esta máquina virtual tiene la protección de BPDU habilitada, el puerto tiene error desactivado y las máquinas virtuales y los adaptadores de VMkernel que usan el adaptador físico del host ya no pueden comunicarse con la red externa.

Si la directiva de formación de equipos y conmutación por error del grupo de puertos contiene más vínculos superiores activos, el tráfico de BDPU se mueve al adaptador para el siguiente vínculo superior activo. El puerto del nuevo conmutador físico se desactiva y más cargas de trabajo no pueden intercambiar paquetes con la red. Finalmente, casi todas las entidades en el host ESXi podrían quedar inaccesibles.

Si la máquina virtual se ejecuta en un host que forma parte de un clúster de vSphere HA y el host queda aislado de la red debido a que la mayoría de los puertos del conmutador físico conectados a él están deshabilitados, el host principal activo en el clúster mueve la máquina virtual remitente de BPDU a otro host. La máquina virtual comienza a desactivar los puertos del conmutador físico conectados al nuevo host. La migración a través del clúster de vSphere HA finalmente lleva a una DoS acumulada en el clúster completo.

Solución

- Si el software de la VPN debe continuar su trabajo en la máquina virtual, deje que el tráfico salga de la máquina virtual y configure el puerto del conmutador físico de forma individual para que transmita tramas de BPDU.

Dispositivo de red	Configuración
Conmutador distribuido o estándar	Configure la propiedad de seguridad Transmisión falsificada en el grupo de puertos en **Permitir** para que las tramas de BPDU puedan abandonar el host y llegar al puerto del conmutador físico. Puede aislar la configuración y el adaptador físico para el tráfico de la VPN colocando la máquina virtual en un grupo de puertos separado y asignando el adaptador físico al grupo. **Precaución** Si se configura la propiedad de seguridad Transmisión falsificada en **Aceptar** para que habilite un host a fin de que envíe tramas de BPDU, ello implica un riesgo de seguridad, ya que una máquina virtual en riesgo puede realizar ataques de suplantación.
Conmutador físico	■ Mantenga Puerto rápido habilitado. ■ Habilite el filtro de BPDU en el puerto individual. Cuando una trama de BPDU llega al puerto, se filtra. **Nota** No habilite el filtro de BPDU a nivel global. Si lo hace, el modo Puerto rápido se deshabilita y todos los puertos del conmutador físico realiza el conjunto completo de funciones de STP.

- Para implementar un dispositivo puente entre dos NIC de máquina virtual conectadas a la misma red de capa 2, deje que el tráfico de BPDU salga de las máquinas virtuales y desactive las características de prevención de bucle Puerto rápido y BPDU.

Dispositivo de red	Configuración
Conmutador distribuido o estándar	Configure la propiedad Transmisión falsificada de la directiva de seguridad en los grupos de puertos en **Aceptar** para permitir que las tramas de BPDU abandonen el host y lleguen al puerto del conmutador físico. Puede aislar la configuración y uno o más adaptadores físicos para el tráfico de puente mediante la colocación de la máquina virtual en un grupo de puertos separado y la asignación de adaptadores físicos al grupo. **Precaución** Si se configura la propiedad de seguridad Transmisión falsificada en **Aceptar** para que habilite la implementación del puente, ello implica un riesgo de seguridad, ya que una máquina virtual en riesgo puede realizar ataques de suplantación.
Conmutador físico	■ Deshabilite Puerto rápido en los puertos hacia el dispositivo de puente virtual para ejecutar STP en ellos. ■ Deshabilite la protección de BPDU y filtre en los puertos que apuntan hacia el dispositivo de puente.

- Proteja el entorno contra ataques de DoS en cualquier caso mediante la activación del filtro de BPDU en el host ESXi o en el conmutador físico.
  - En un host que ejecuta ESXi 4.1 Update 3, ESXi 5.0 Patch 04 y versiones posteriores a la 5.0 y ESXi 5.1 Patch 01 y versiones posteriores, habilite el filtro BPDU invitado de una de las siguientes formas y reinicie el host:
    - En la pestaña **Configurar** del host de la tabla Configuración avanzada del sistema en vSphere Web Client, establezca la propiedad Net.BlockGuestBPDU en **1**.
    - En ESXi Shell para el host, escriba el siguiente comando de vCLI:

      ```
      esxcli system settings advanced set -o /Net/BlockGuestBPDU -i 1
      ```

  - En un host que no tiene el filtro BPDU invitado implementado, habilite el filtro de BPDU en el puerto del conmutador físico para el dispositivo de puente virtual.

Dispositivo de red	Configuración
Conmutador distribuido o estándar	Configure la propiedad Transmisión falsificada de la directiva de seguridad en el grupo de puertos en **Rechazar**.
Conmutador físico	■ Mantenga la configuración de Puerto rápido. ■ Habilite el filtro de BPDU en el puerto del conmutador físico individual. Cuando una trama de BPDU llega al puerto físico, se filtra. **Nota** No habilite el filtro de BPDU a nivel global. Si lo hace, el modo Puerto rápido se deshabilita y todos los puertos del conmutador físico realiza el conjunto completo de funciones de STP.

Baja capacidad de proceso para cargas de trabajo UDP en máquinas virtuales Windows

Cuando una máquina virtual Windows en vSphere 5.1 y versiones posteriores transmite paquetes de UDP grandes, la capacidad de proceso es menor de la esperada o es oscilante cuando otro tráfico es insignificante.

Problema

Cuando una máquina virtual transmite paquetes de UDP mayores de 1024 bytes, usted experimenta una capacidad de proceso menor de la esperada u oscilante incluso cuando otro tráfico es insignificante. En caso de un servidor de transmisión de vídeo, se pausa la reproducción del vídeo.

Causa

Para cada paquete de UDP mayor a 1024 bytes, la pila de red Windows espera una interrupción en la realización de la transmisión antes de enviar el siguiente paquete. A diferencia de versiones anteriores, vSphere 5.1 y versiones posteriores no ofrecen una solución alternativa clara para el problema.

Solución

- Aumente el umbral en bytes en el cual Windows cambia su comportamiento para paquetes de UDP a través de la modificación del registro del sistema operativo invitado de Windows.

  a Busque la clave de registro `HKLM\System\CurrentControlSet\Services\Afd\Parameters`.

  b Agregue un valor con el nombre `FastSendDatagramThreshold` del tipo DWORD igual a 1500.

  Para obtener información sobre cómo solucionar este problema en el registro de Windows, consulte http://support.microsoft.com/kb/235257.

- Modifique la configuración de combinación de la NIC de la máquina virtual.

  Si la máquina virtual Windows tiene un adaptador de vNIC VMXNET3, configure uno de los siguientes parámetros en el archivo `.vmx` de la máquina virtual. Use vSphere Web Client o modifique directamente el archivo `.vmx`.

Acción	Parámetro	Valor
Aumente la tasa de interrupciones de la máquina virtual a una tasa superior a la tasa de paquetes esperada. Por ejemplo, si la tasa del paquete esperada es de 15.000 interrupciones por segundo, configure la tasa de interrupciones en 16.000 interrupciones por segundo. Configure el parámetro `ethernetX.coalescingScheme` en **`rbc`** y el parámetro `ethernetX.coalescingParams` en **`16000`**. La tasa de interrupciones predeterminada es de 4.000 interrupciones por segundo.	`ethernetX.coalescingScheme` `ethernetX.coalescingParams`	rbc 16000
Deshabilite la combinación para baja capacidad de proceso o cargas de trabajo sensibles a latencia. Para obtener información sobre cómo configurar cargas de trabajo de baja latencia, consulte Prácticas recomendadas para ajuste de rendimiento de cargas de trabajo sensibles a latencia en máquinas virtuales vSphere.	`ethernetX.coalescingScheme`	deshabilitado
Revierta al algoritmo de combinación de las versiones anteriores de ESXi. **Nota** La capacidad de revertir al algoritmo anterior no estará disponible en versiones posteriores de vSphere.	`ethernetX.coalescingScheme`	calibrar

  X junto a `ethernet` representa el número de secuencia de la vNIC en la máquina virtual.

  Para obtener más información sobre cómo configurar parámetros en el archivo `.vmx`, consulte el documento *Administrar máquinas virtuales de vSphere*.

- Modifique la configuración de combinación del host ESXi.

  Este enfoque afecta a todas las máquinas virtuales y todas las NIC de máquinas virtuales en el host.

  Puede editar la lista de parámetros de configuración avanzada del sistema para el host en vSphere Web Client o mediante el uso de un comando de consola vCLI en el host desde ESXi Shell.

Acción	Parámetro en vSphere Web Client	Parámetro para el comando **esxcli system settings sdvanced set**	Valor
Configure una tasa de interrupciones predeterminada mayor que la tasa de paquetes esperada. Por ejemplo, configure la tasa de interrupciones en 16.000 en caso de que se esperen 15.000 interrupciones por segundo.	`Net.CoalesceScheme` `Net.CoalesceParams`	`/Net/CoalesceScheme` `/Net/CoalesceParams`	rbc 16000
Deshabilite la combinación para baja capacidad de proceso o cargas de trabajo sensibles a latencia. Para obtener información sobre cómo configurar cargas de trabajo de baja latencia, consulte Prácticas recomendadas para ajuste de rendimiento de cargas de trabajo sensibles a latencia en máquinas virtuales vSphere.	`Net.CoalesceDefaultOn`	`/Net/CoalesceDefaultOn`	0
Revierta el esquema de combinación de las versiones anteriores de ESXi. **Nota** La capacidad de revertir al algoritmo anterior no estará disponible en versiones posteriores de vSphere.	`Net.CoalesceScheme`	`/Net/CoalesceScheme`	calibrar

Para obtener información sobre cómo configurar un host desde vSphere Web Client, consulte la documentación de *Administrar vCenter Server y hosts*. Para obtener información sobre cómo configurar propiedades del host usando un comando vCLI, consulte la documentación de *Referencia de vSphere Command-Line Interface*.

Las máquinas virtuales en el mismo grupo de puertos distribuido y en diferentes hosts no pueden comunicarse entre sí

En ciertas condiciones, las máquinas virtuales que se encuentran en el mismo grupo de puertos distribuido, pero en diferentes hosts no pueden comunicarse entre sí.

Problema

Máquinas virtuales que se encuentran en diferentes hosts y en el mismo grupo de puertos no pueden comunicarse. Los pings desde una máquina virtual a otra no surten efecto. No puede migrar las máquinas virtuales entre los hosts utilizando vMotion.

Causa

- No hay NIC físicas en algunos de los hosts asignados a vínculos superiores activos o en espera en el orden de formación de equipos y conmutación por error del grupo de puertos distribuido.

- Las NIC físicas en los hosts que están asignados a los vínculos superiores activos o en espera se encuentran en diferentes VLAN en el conmutador físico. Las NIC físicas en diferentes VLAN no pueden verse entre sí y, por lo tanto, no pueden comunicarse entre sí tampoco.

Solución

- En la topología del conmutador distribuido, compruebe cuál host no tiene NIC físicas asignadas a un vínculo superior activo o en espera en el grupo de puertos distribuido. Asigne al menos una NIC física en ese host a un vínculo superior activo en el grupo de puertos.
- En la topología del conmutador distribuido, compruebe los identificadores de VLAN de las NIC físicas que están asignadas a los vínculos superiores activos en el grupo de puertos distribuido. En todos los hosts, asigne NIC físicas que sean de la misma VLAN a un vínculo superior activo en el grupo de puertos distribuido.
- Para verificar que no exista ningún problema en la capa física, migre las máquinas virtuales al mismo host y compruebe la comunicación entre ellas. Compruebe que el tráfico ICMP entrante y saliente se encuentre habilitado en el sistema operativo invitado. De forma predeterminada, el tráfico ICMP se encuentra deshabilitado en Windows Server 2008 y Windows Server 2012.

Error al intentar encender una vApp migrada debido a que falta el perfil de protocolo asociado

No puede encender una a vApp o máquina virtual que transfirió a un centro de datos o un sistema de vCenter Server porque falta un perfil de protocolo de red.

Problema

Después de realizar una migración en frío de una vApp o una máquina virtual a otro centro de datos o sistema de vCenter Server, se produce un error al intentar encenderla. Un mensaje de error indica que no se puede inicializar o asignar una propiedad porque la red de la vApp o máquina virtual no tiene un perfil de protocolo de red asociado.

```
No es posible inicializar la propiedad 'property'. La red 'port group' no tiene un perfil de protocolo de red asociado.
```

```
No es posible asignar una dirección IP para la propiedad 'property'. La red 'port group' no tiene un perfil de protocolo de red asociado.
```

Causa

Mediante el uso del entorno de OVF, la vApp o máquina virtual recupera configuración de red de un perfil de protocolo de red que está asociado con el grupo de puertos de la vApp o máquina virtual.

vCenter Server crea dicho perfil de protocolo de red para usted cuando instala el OVF de una vApp y asocia el perfil con el grupo de puertos que especifica durante la instalación.

La asignación entre el perfil de protocolo y el grupo de puertos es válido solo en el ámbito de un centro de datos. Cuando mueve la vApp, el perfil de protocolo no se transfiere al centro de datos de destino debido a los siguientes motivos:

- Es posible que la configuración de red del perfil de protocolo no esté disponible en el entorno de red del centro de datos de destino.
- Puede que en el centro de datos ya exista un grupo de puertos que tiene el mismo nombre y está asociado con otro protocolo de red, y las vApps y máquinas virtuales podrían estar conectadas a este grupo. El reemplazo de los perfiles de protocolo para el grupo de puertos podría afectar la conectividad de estas vApp y máquinas virtuales.

Solución

- Cree un perfil de protocolo de red en el centro de datos o sistema de vCenter Server de destino con la configuración de red requerida y asocie el perfil de protocolo con el grupo de puertos al cual se conecta la vApp o máquina virtual. Por ejemplo, este enfoque es adecuado si la vApp o máquina virtual es una extensión de vCenter Server que utiliza vCenter Extension vService.

  Para obtener información acerca de cómo proporcionar configuración de red para una vApp o máquina virtual desde un perfil de protocolo de red, consulte la documentación de *Redes de vSphere*.
- Use vSphere Web Client para exportar el archivo de OVF de la vApp o máquina virtual desde el centro de datos o sistema de vCenter Server de origen e impleméntelo en el centro de datos o sistema de vCenter Server de destino.

  Cuando usa vSphere Web Client para implementar el archivo de OVF, el sistema de vCenter Server de destino crea el perfil de protocolo de red para la vApp.

  Para obtener información sobre cómo administrar archivos de OVF en vSphere Web Client, consulte la documentación de *Administrar máquinas virtuales de vSphere*.

La operación de configuración de redes se revierte y un host se desconecta de vCenter Server

Cuando intenta agregar o configurar redes en vSphere Distributed Switch en un host, la operación se revierte y el host se desconecta de vCenter Server.

Problema

En vSphere 5.1 o una versión posterior, un intento por realizar una operación de configuración de redes en vSphere Distributed Switch en un host, como la creación de un adaptador de máquina virtual o un grupo de puertos, hace que el host se desconecte de vCenter Server y redunda en el mensaje de error `La transacción se ha revertido en el host`.

Causa

En condiciones estresantes en un host, es decir, si muchas operaciones de redes simultáneas compiten por recursos limitados, el tiempo para realizar algunas de las operaciones podría superar el tiempo de espera predeterminado para revertir operaciones de configuración de red en el conmutador distribuido. Como resultado, estas operaciones se revierten.

Por ejemplo, dicha condición podría surgir cuando crea un adaptador de VMkernel en un host que tiene un número muy alto de puertos de interruptor o adaptadores virtuales, todos los cuales consumen recursos del sistema en el host.

El tiempo de espera predeterminado para revertir una operación es de 30 segundos.

Solución

- Use vSphere Web Client para aumentar el tiempo de espera para reversión en vCenter Server.

  Si vuelve a encontrar el mismo problema, aumente el tiempo de espera de reversión en 60 segundos gradualmente hasta que la operación tenga suficiente tiempo para realizarse correctamente.

  a En la pestaña **Configurar** de una instancia de vCenter Server, expanda **Configuración**.

  b Seleccione **Configuración avanzada** y haga clic en **Editar**.

  c Si la propiedad no está presente, agregue el parámetro `config.vpxd.network.rollbackTimeout` a la configuración.

  d Escriba un nuevo valor, en segundos, para el parámetro `config.vpxd.network.rollbackTimeout`

  e Haga clic en **Aceptar**.

  f Reinicie el sistema de vCenter Server para aplicar los cambios.

- Aumente el tiempo de espera para la reversión editando el archivo de configuración `vpxd.cfg`.

  Si vuelve a encontrar el mismo problema, aumente el tiempo de espera de reversión en 60 segundos gradualmente hasta que la operación tenga suficiente tiempo para realizarse correctamente.

  a En una instancia de vCenter Server, desplácese al directorio que contiene el archivo de configuración `vpxd.cfg`.

    - En un sistema operativo Windows Server, desplácese hasta *directorio de inicio de vCenter Server*`\Application Data\VMware\VMware VirtualCenter`.
    - En vCenter Server Appliance, desplácese a `/etc/vmware-vpx`.

  b Abra el archivo `vpxd.cfg` para editarlo.

c En la sección `<network>`, aumente el tiempo de espera en el elemento `<rollbackTimeout>`.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

d Guarde y cierre el archivo.

e Reinicie el sistema de vCenter Server para aplicar los cambios.

Solucionar problemas de licencias

9

Los temas de solución de problemas de licencias ofrecen soluciones a posibles problemas que se podrían encontrar como resultado de una configuración de licencia incorrecta o incompatible en vSphere.

Este capítulo incluye los siguientes temas:

Solucionar problemas de licencias del host

Es posible que se encuentren diferentes problemas producto de una configuración de licencia incompatible o incorrecta de hosts ESXi.

No se puede asignar una licencia a un host ESXi

En ciertas condiciones, es posible que no pueda asignar una licencia a un host ESXi.

Problema

Intenta asignar una licencia a un host ESXi, pero no puede realizar la operación y recibe un mensaje de error.

Causa

Es posible que no pueda asignar una licencia a un host ESXi debido a los siguientes motivos:

- El uso calculado de licencias para el host supera la capacidad de licencias. Por ejemplo, tiene una clave de licencia de vSphere con capacidad para dos CPU. Intenta asignar la clave a un host que tiene cuatro CPU. No puede asignar la licencia, porque el uso de licencias necesario para el host es mayor que la capacidad de licencias.
- Las características en el host no coinciden con la edición de la licencia. Por ejemplo, podría configurar hosts con vSphere Distributed Switch y vSphere DRS mientras están en modo de evaluación. Posteriormente, intenta asignar la licencia de vSphere Standard a los hosts. Esta operación genera errores debido a que vSphere Standard Edition no incluye vSphere Distributed Switch ni vSphere DRS.

- El host está conectado a un sistema de vCenter Server que tiene asignado a una licencia que restringe la edición de la licencia que desea asignar.

Solución

- Asigne una licencia con mayor capacidad.
- Actualice la edición de la licencia para que coincida con los recursos y las características del host, o deshabilite las características y los recursos que no coinciden con la edición de la licencia.
- Asigne una licencia de vSphere cuya edición no sea compatible con la edición de licencia de vCenter Server.

El host ESXi se desconecta de vCenter Server

Un host ESXi podría desconectarse de vCenter Server o todos los hosts ESXi podrían desconectarse de vCenter Server al mismo tiempo.

Problema

Un host ESXi se desconecta de vCenter Server cuando el período de evaluación o la licencia del host caducan. Todos los hosts ESXi se desconectan de vCenter Server cuando el período de evaluación o la licencia de vCenter Server caducan. Se recibe un mensaje de error relacionado con licencias tanto cuando se desconecta un host individual como cuando se desconectan todos los hosts. No puede agregar hosts al inventario de vCenter Server. Los hosts y las máquinas virtuales en los hosts siguen ejecutándose.

Causa

- El período de evaluación de 60 días del host o la licencia del host han caducado.
- El período de evaluación de 60 días de vCenter Server o la licencia de vCenter Server han caducado.

Solución

- Asigne una licencia de vSphere al host ESXi e intente volver a conectarlo a vCenter Server.
- Asigne una licencia de vCenter Server al sistema devCenter Server.

No es posible encender una máquina virtual

Intenta encender una máquina virtual, pero la operación no es correcta y recibe un mensaje de error.

Problema

No puede encender una máquina virtual en un host ESXi.

Causa

Es posible que no pueda encender una máquina virtual debido a los siguientes motivos.

- El período de evaluación de 60 días del host ha caducado.
- La licencia del host caducó.

Solución

Tabla 9-1. Encender una máquina virtual

Motivo	Solución
El período de evaluación del host caducó.	Asigne una licencia de vSphere al host ESXi.
La licencia del host caducó.	Asigne una licencia de vSphere al host ESXi.

No se puede configurar o utilizar una característica

No se puede usar una característica ni cambiar su configuración.

Problema

No puede usar o configurar una característica y aparece un mensaje de error relacionado con licencias.

Causa

Se asignó una licencia al host ESXi o al sistema vCenter Server que no admite las características que se desean configurar.

Solución

Compruebe las características con licencia en el host ESXi y el sistema vCenter Server. Actualice la edición de la licencia asignada al host o vCenter Server en caso de que no incluyan las características que intenta configurar o usar.